Titre: Title:	Sécurisation des VANETS par la méthode de réputation des noeuds
Auteur: Author:	Richard Engoulou
Date:	2013
Type:	Mémoire ou thèse / Dissertation or Thesis
Référence: Citation:	Engoulou, R. (2013). Sécurisation des VANETS par la méthode de réputation des noeuds [Master's thesis, École Polytechnique de Montréal]. PolyPublie. https://publications.polymtl.ca/1100/

URL de PolyPublie: PolyPublie URL:	https://publications.polymtl.ca/1100/
Directeurs de recherche: Advisors:	Martine Bellaïche, & Samuel Pierre
Programme: Program:	Génie informatique

UNIVERSITÉ DE MONTRÉAL

SÉCURISATION DES VANETS PAR LA MÉTHODE DE RÉPUTATION DES NOEUDS

RICHARD ENGOULOU

DÉPARTEMENT DE GÉNIE INFORMATIQUE ET GÉNIE LOGICIEL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

MÉMOIRE PRÉSENTÉ EN VUE DE L'OBTENTION

DU DIPLÔME DE MAÎTRISE ÈS SCIENCES APPLIQUÉES

(GÉNIE INFORMATIQUE)

AVRIL 2013

UNIVERSITÉ DE MONTRÉAL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

Ce mémoire intitulé:

SÉCURISATION DES VANETS PAR LA MÉTHODE DE RÉPUTATION DES NŒUDS

présenté par : ENGOULOU Richard

en vue de l'obtention du diplôme de : Maîtrise ès Sciences Appliquées

a été dûment accepté par le jury d'examen constitué de :

Mme HANIFA Boucheneb, Doctorat, présidente

Mme BELLAÏCHE Martine, Ph.D., membre et directrice de recherche

M. PIERRE Samuel, Ph.D., membre et codirecteur de recherche

M. QUINTERO Alejandro, Doct., membre

DÉDICACE

À mes très chers parents,

À mes frères, ma sœur et mes belles-sœurs

À mes amis et amies

À mes collègues du laboratoire LARIM

REMERCIEMENTS

Je tiens à remercier ma directrice de recherche Mme. Martine Bellaïche pour avoir assuré la direction de mes travaux, pour la qualité de son encadrement, ses remarques pertinentes, son soutien et qui de par son expérience m'a permis de finaliser ce travail grâce à son suivi efficace et ses conseils avisés.

Je tiens aussi à remercier mon co-directeur de recherche M. Samuel Pierre pour avoir assuré la co-direction de mes travaux, pour sa patience, ses remarques toujours pertinentes, pour les remises en questions qui m'ont permis de mieux avancer dans ma recherche.

Merci aussi aux membres du laboratoire de recherche en Informatique mobile (LARIM) que j'ai eu la chance de côtoyer tout au long de mes études aux cycles supérieures. Une mention spéciale doit être portée à mon collègue Moussa Ouédraogo qui m'a prodigué des conseils très utiles dans l'élaboration de mes simulations et qui est devenu un ami avec qui j'espère entretenir une relation à long terme.

Je remercie également tous les professeurs du département du génie Informatique, notamment Guillaume-Alexandre Bilodeau, Samuel Kadoury pour m'avoir donné l'opportunité d'officier en tant que chargé de laboratoire. Il n'y a rien de plus valorisant pour moi que de partager mon savoir avec des étudiants motivés d'apprendre.

Je remercie aussi les membres du jury qui ont accepté de réviser et d'évaluer ce mémoire.

Une pensée particulière est adressée à mes frères, mes amies et amis qui m'ont impulsé dans la poursuite de mes études et qui ont été à mes côtés tout au long de la période d'étude même lorsque c'était difficile pour moi. Je ne vous remercierez jamais assez.

Un merci particulier à celle qui a toujours été là pour moi, malgré la distance qui nous a séparé, tu n'as pas cessé de m'encourager, tu es pour moi un rock, merci mon amour.

Merci à tous.

RÉSUMÉ

Les réseaux ad hoc sans fil véhiculaires (VANET) permettent la communication entre les véhicules et entre les équipements de communication placés le long des rues. Cette communication apporte plusieurs avantages. Le premier est l'augmentation de la sécurité routière. Le second est l'agrémentation de l'expérience de conduite et de voyage. La sécurité routière est assurée par une catégorie d'applications dites « applications de sécurité du trafic routier ». La seconde catégorie d'application considérée regroupe les applications liées au confort des usagers sur la route, telles que : l'accès à une connexion Internet durant le voyage, le téléchargement de contenu multimédia, les jeux en ligne et en réseau, les applications de paiement pour les services. La troisième catégorie d'applications regroupe les applications de maintenance à distance. Toutes ces applications nécessitent que les communications soient sécurisées. Cette contrainte est d'autant plus importante pour les applications de sécurité du trafic, car les informations transmises par ces applications peuvent mener au changement du comportement des automobilistes et conduire à des situations aussi catastrophiques que les accidents de la circulation.

Depuis quelques années, plusieurs travaux ont été menés, tant par l'industrie automobile que par les universités ou encore les institutions de recherche gouvernementales en vue de sécuriser les VANETS. De ces travaux, plusieurs méthodes ont émergé, parmi lesquelles, les méthodes cryptographiques à clé publique/privée, les méthodes de sécurisation des protocoles de communication, les méthodes de sécurisation par révocation de certificat, les méthodes de sécurisation par réputation. Cette dernière méthode permet de vérifier les variables telles que la vitesse, l'accélération, la position géographique, le rayon de transmission, la direction, etc. Afin d'empêcher les adversaires de mentir et d'induire les automobilistes en erreur provoquant des accidents ou du trafic sur certains tronçons de route. C'est pourquoi l'objectif de notre travail est de doter les nœuds hôtes d'un système de réputation qui servira de cadre d'analyse des différentes variables publiées par les véhicules émetteurs. Cette analyse permet de filtrer les nœuds qui fournissent des variables erronées sur leur position géographique, leur vitesse ou encore leur accélération. Ces informations sont importantes car pour la majorité des applications de sécurité du trafic, le nœud hôte se fie à elles pour poser des actions à propos d'une alerte de danger reçue par d'autres nœuds (accident, risque de collision, mauvais état de la route, risque de trafic, etc.).

Notre système réalise des tests sur les variables reçues pour se rassurer qu'elles concordent avec les paramètres attendues. Ces paramètres sont données par les observations faites grâces aux capteurs, aux récepteurs GPS et aux équipements de communication embarqués sur les véhicules, ou encore grâce à des calculs effectués pendant la réception des variables. Notre première contribution dans ce travail est la conception d'un système de filtrage, qui permet de supprimer tous les messages pour lesquels les variables sont erronées et ainsi de détecter et d'éjecter du réseau les adversaires potentiels. Notre seconde contribution est de doter notre système d'une capacité de réhabilitation des nœuds adversaires par le passé et qui se comportent maintenant de façon exemplaire. Notre troisième contribution est la mise en place d'un système à deux niveaux : un premier niveau binaire, rigide qui ne permet pas une réhabilitation, et un second niveau qui introduit la flexibilité, et la réhabilitation tout en permettant aux utilisateurs de le personnaliser lors de l'implémentation. Notre quatrième contribution est d'avoir pu modifier le protocole AODV dans le simulateur Network Simulator (NS-2) dans sa deuxième version, afin de réaliser des simulations réalistes à propos du système de réputation que nous proposons.

Mots clés : Sécurité, Réseaux sans fil véhiculaire, système de réputation.

ABSTRACT

Vehicular ad-hoc network is a specific type of Mobile ad-hoc network (MANET) that provides communication between nearby vehicles and nearby roadside equipments. This communication provides several advantages. The first one is to increase road safety. The second one is the improvement of the driving experience. Road safety is ensured by applications category called “safety applications”. The second category includes comfort applications of road users, such as access to an Internet connection during the trip, downloading multimedia content, online and network gaming, tool payment services. The third category includes remote maintenance applications. All these applications require efficient secured communication. This constraint is particularly important for safety applications, as the information transmitted by these applications can lead to drivers’ behavior changing and caused catastrophic situations such as cars’ accidents.

In recent years, several studies have been conducted, both in the automotive industry and universities or government researches’ institutions to secure VANETs. From all these researches several VANETS’ security methods have emerged, including the public/private key cryptographic methods, communication protocols’ security methods, certificate revocation methods, reputation methods and so one. The reputation method is used to check information such as speed, acceleration, location, transmission range, direction, etc. To prevent attacks from malicious nodes that would lie about the variables that they are publishing to mislead motorists’ behavior and cause cars’ accidents or traffic jam on certain stretches of road. That is why the objective of our work is to provide hosts nodes with a reputation system to check different variables published by transmitting nodes. This analysis allows filtering nodes that publish false information about their geographical position, speed or acceleration. This information is important because, for the majority of safety applications, the host node relies on them and the motorist will react considering them. Our system performs tests on the information received to make sure that they are consistent with the expected parameters. These parameters are given by observations thanks to sensors, GPS receivers and vehicles’ communication equipments on board. Our first contribution in this work is the design of a filter system that removes all messages whose variables are erroneous and thus to detect and eject potential adversaries out of the network. Our second contribution is to provide our system with a capacity of rehabilitation of

nodes that were previously regarded as adversaries who now behave in an exemplary manner. Our third contribution is the establishment of a two-tier system, a first binary level and a second level which introduces flexibility and allows users to customize them during the implementation. Our fourth contribution is to be able to modify the AODV protocol in NS-2 simulator to test our reputation system for realistic simulations.

Keywords: Security, vehicular ad hoc networks, reputation.

TABLE DES MATIÈRES

LISTE DES TABLEAUX

LISTE DES FIGURES

LISTE DES SIGLES ET ABRÉVIATIONS

CA	Certificate Authority
CA	Comfort and maintenance Applications
CACC	Collaborative Adaptive Cruise Control
CORE	Collaborative Reputation Mechanism to enforce node cooperation in Mobile Ad Hoc Networks
DSRC	Dedicated Short Range Communication
EDR	Event Data Recorder
EEBL	Emergency Electronic Brake Lights
ELP	Electronic License Plate
EO	Event Observer
EP	Event Participant
ER	Event Reporter
FCC	Federal Communications Commission
GMs	Group Managers
GPS	Global Positioning System
ITA	Intelligent Transport Applications
ITS	Intelligent Transportation System
LEAS	Law Enforcement Authorities
MAC	Message Authentication Code
MANETs	Mobile Ad-hoc Networks
NAs	Network Authorities
OBU	On Board Unit
PKI	Public Key Infrastructure

RSU	Road Side Infrastructure
RTAs	Regional Transportation Authorities
SAV	Security Architecture for VANET
SPAT	Signal Phase And Timing
SSVR	Système de Sécurisation des VANETS par Réputation
TEA	Transport Efficiency Applications
TGS	Ticket Granting Service
TGT	Ticket Granting Ticket
TPD	Tamper Proof Device
TPM	Trusted Platform Module
TSA	Transport Safety Application
TTP	Trusted Third Party
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
VC	Vehicular Communications
VANETs	Vehicular Ad-hoc Networks
VSC	Vehicle Safety Communication
WLAN	Wireless Local Ad-hoc Network

CHAPITRE 1

INTRODUCTION

Notre mémoire s'intéresse à la sécurisation des VANETs par la méthode de réputation des nœuds, nous proposons un système de réputation qui sert de cadre d'analyse des variables reçues par le nœud récepteur en provenance du nœud émetteur. Ce système permet au nœud récepteur de n'accepter que des informations provenant des nœuds honnêtes.

Ce chapitre s'articule en quatre parties qui sont successivement, (i) le contexte d'une attaque dans un environnement VANET, (ii) les défenses mises en place pour empêcher ces attaques, (iii) l'esquisse de la méthodologie de notre solution de défense proposée, (iv) enfin le plan de ce mémoire.

1.1 Contexte

Les VANETS sont des réseaux pour lesquelles les nœuds de communications sont des véhicules. Ces réseaux améliorent particulièrement la sécurité du trafic sur la route et globalement, la sécurité du système de transport grâce à des applications dites de sécurité. Ils améliorent aussi l'expérience de conduite grâce à des applications dites de confort. Les communications se déroulent d'une part entre les infrastructures placées le long des rues et les véhicules et d'autres parts entre les véhicules entre eux. Il existe plusieurs types d'applications selon l'information à transmettre et selon le contexte. Nous présentons ici quelques-unes des applications liées à la sécurité du trafic. Il s'agit de : l'application d'avertissement de la violation des feux de signalisation, l'application d'avertissement à l'approche d'un tournant, l'application de lumière d'indication d'un freinage d'urgence, l'application d'avertissement coopératif d'une collision imminente, l'application d'avertissement de changement de voie, etc. Toutes les applications que nous venons de citer ont pour caractéristique commune qu'elles dépendent des variables publiées par le véhicule qui initie la communication. En effet lorsqu'un véhicule reçoit une alerte ou un avertissement, il exploite les informations publiées par l'émetteur telles que sa vitesse, sa position géographique, son accélération, sa direction ou encore son rayon de transmission. Grâce à ces informations et le type d'alerte reçue, le conducteur du véhicule récepteur peut réagir efficacement pour éviter un accident ou une situation dangereuse.

1.2 Éléments de la problématique

Le véhicule récepteur exploite les informations publiées par le véhicule émetteur, afin de mieux analyser les situations qui se présentent. Cette situation peut donner lieu à des attaques de sécurité par des adversaires qui peuvent avoir pour objectifs de rendre le réseau non-fonctionnel, de causer un accident ou encore cibler une voiture particulière, afin de nuire à son conducteur. Cette situation présente le problème de la sécurité dans les VANETS. Ces réseaux n'étant pas encore réellement implémentés, plusieurs attaques ont été imaginées parmi les quelles : l'attaque de déni de service qui consiste à rendre le réseau non-fonctionnel, l'attaque d'altération ou de suppression des messages qui consiste à modifier l'intégrité des messages envoyés sur le réseau. Plus récemment une nouvelle attaque a été déterminée, il s'agit de l'attaque d'illusion. Cette attaque consiste à publier des variables erronées sur la position géographique, la vitesse, l'accélération, la direction, la distance et une alerte qui induira en erreur le conducteur de l'automobile récepteur. Car le véhicule récepteur exploite toutes ces variables afin de déterminer comment se comporter face à l'alerte reçue. Cette attaque peut causer des dommages important allant d'une simple collision à un accident très grave.

La problématique de notre étude est de mettre en place un système de réputation qui servira de cadre d'analyse afin de détecter les adversaires potentiels qui mentent sur les variables qu'ils publient.

1.3 Objectifs de la recherche

L'objectif général de cette recherche est de proposer un cadre d'analyse du comportement des autres véhicules du VANET par des métriques afin d'éviter des attaques de manipulation des informations échangées sur le réseau. De manière plus spécifique, ce mémoire vise à :

1. Proposer un système de réputation fiable qui joue le rôle de cadre d'analyse du comportement des autres véhicules du VANET par des métriques afin d'éviter des attaques des nœuds qui mentent sur les variables publiées afin de nuire à la bonne marche du réseau;
2. Construire des métriques qui permettent d'évaluer la fiabilité d'un nœud dans le réseau;

3. Intégrer les notes obtenues par ces métriques afin d'obtenir un score global de réputation qui tienne compte non seulement du score défini par le nœud récepteur mais aussi des témoignages fournis par les nœuds voisins;
4. Évaluer les performances de notre système de réputation en utilisant le simulateur NS-2 (Network Simulator).

1.4 Esquisse de la méthodologie

Nous proposons dans ce mémoire un système de réputation qui permet de filtrer les véhicules malveillants qui tentent de fournir des variables erronées à propos de leur position géographique, leur vitesse et toutes les autres variables nécessaire au véhicule récepteur par rapport à la réaction à avoir à la suite d'un avertissement ou d'une alerte visant à aider les automobilistes à éviter des accidents ou d'autres situations malencontreuses. Cette approche repose sur la construction de métrique mathématiques qui permettent de vérifier les variables reçues par les véhicules émetteurs. Chaque variable testée donne lieu à une note comprise entre 0 et 1 inclusivement, selon que la métrique est vérifiée ou non. L'ensemble des notes est ensuite agrégé pour construire le score local de réputation. Nous prenons aussi en considération les témoignages des véhicules voisins qui représentent les scores de réputation du véhicule émetteur par rapport aux véhicules voisins. L'agrégation du score local de réputation et les témoignages constitue le score global de réputation. C'est ce dernier score qui permet au système de réputation de décider d'accepter ou de supprimer le message reçu. Grâce à cette approche, nous pouvons non seulement détecter les véhicules qui mentent sur les variables qu'elles fournissent mais aussi les éjecter du VANET.

1.5 Plan du mémoire

Ce mémoire est composé de sept chapitres. Le chapitre 1 est l'introduction qui présente les divers aspects de ce travail : contexte, objectif, méthodologie et plan du mémoire. Le chapitre 2 présente un état de l'art de la sécurité dans les VANETs. Le chapitre 3 présente le concept de réputation de façon générale et dans les réseaux mobiles. Le chapitre 4 présente le système de réputation que nous proposons. Au chapitre 5, nous présentons l'évaluation des performances de notre système de réputation et les résultats des simulations réalisées. Dans le chapitre 6, nous

concluons notre travail et nous présentons les limites de notre recherche, les contributions apportées et les travaux futurs à réaliser pour améliorer notre système de réputation.

CHAPITRE 2

ÉTAT DE L'ART DE LA SÉCURITÉ DANS LES VANETS

Les réseaux ad-hoc véhiculaires (VANETs) sont un type spécifique de réseaux ad-hoc mobile (MANET), qui permettent la communication entre les véhicules sur la route et les équipements de communication placés le long des routes [1, 2]. Dans ce type de réseaux, les véhicules sont considérés comme des nœuds de communication capable de faire partie d'un réseau auto-organisé sans connaissance préalable les uns des autres[3]. Ainsi, l'on peut définir deux catégories d'équipement : les équipements internes au véhicules (On Board Unit :OBU) et les équipement externe aux véhicules (Road Side Unit : RSU). Les "OBUs" sont donc des équipements radio installés dans les véhicules. Les "RSUs" par contre sont place au bord des route et constitue l'infrastructure réseau, ils sont d'ailleurs utilisé comme des routeurs entre les véhicules. Les "OBUs" utilisent les signaux DSRC(Dedicated Short Range Communication) pour communiquer avec les « RSU » [4].

Les VANETs sont devenues l'une des technologies sans fil les plus pertinentes. Ils constituent l'une des approches les plus prometteuses pour l'implémentation des systèmes de transport intelligents (ITS). Les VANETs diffèrent des MANETs de plusieurs façons: la haute mobilité des nœuds, la grande échelle des réseaux, les contraintes géographiques de la topologie, la topologie hautement dynamique, les contraintes élevées du temps réel, la connectivité sporadique du réseau, la lenteur du déploiement, la non-fiabilité des canaux de communication, etc.[1, 2, 5]. L'objectif premier c'est de permettre la communication entre les véhicules. De ce fait, il est nécessaire que ces véhicules incorporent des équipements et des interfaces de communications et un rayon spectral de communication dédié aux échanges dans un VANET.

Dans le but de faire partie de façon effective du réseau, les véhicules ont besoin des équipements qui leur permettent d'observer et de conserver les informations de leur environnement, d'informer leurs voisins, et de prendre des décisions au vu des informations récemment collectées. Ces équipements peuvent être: les récepteurs GPS(Global Positioning System), les radars, les capteurs, les enregistreurs d'évènement (EventData Recorder EDR) et des antennes omnidirectionnelles [6].

Les VANETs ont été conçus pour apporter un certain nombre d'avantages, tel que: la réduction des accidents de la circulation sur les routes, du confort de conduit et de voyage pour les conducteurs et les passagers, des moyens de paiement facilité pour certains services tel les parking, du gaz, etc. Ces réseaux implémentent aussi des applications de sureté, de maintenance et de confort comme l'accès à une connexion Internet, les jeux en ligne et en réseau, les téléchargement de matériel audio et vidéo [7]. Toutes ces applications font appel à l'échange des messages comme les messages d'urgences, les avertissements sur les incidents survenus, sur les conditions de la route à des instants précis, et les informations d'aide à la conduite. Tous ces échanges font intervenir des données informatiques et le contenu des messages peut influer sur le comportement des conducteurs et ainsi changer la topologie du réseau. Ceci implique donc un risque de danger d'attaque par des usagers malveillants qui peuvent trafiquer les messages échangés sur le réseau [8]. Quelques attaques que l'on peut observer sur les VANETs sont : des attaques de blocage de la circulation, attaque de rejeux, attaque de mensonge sur les informations transmises, les attaques de déni de service, les attaques de mascarade, attaque de vol d'identité, attaque d'illusion, attaque sur les équipements de communication, etc. [2]. Un autre challenge auquel les concepteurs des VANETs doivent faire face, c'est la vie privé des usagers. Il existe une réticence chez les usagers à laisser leurs informations gérer par une entité centrale qui agirait comme le système « big brother ». D'autres parts, la plupart des solutions proposées pour sécuriser les VANETs exposent la vie privée des usagers.

Ce chapitre est structure de la façon suivante: la section II présente l'architecture des VANETs, la sections III fait référence aux challenges dans les VANETs, dans la section IV, nous discutons des applications dans les VANETs, en section V, les requis de sécurité sont examinés, dans la section VI, nous présentons les menaces dans les VANETs, la section VII présente le profil des attaquants, dans la section VIII, ce sont les caractéristiques des attaques qui sont abordées, la section IX conclut le chapitre.

2.1 Caractéristiques et architecture des VANETs

L'architecture des VANETs peut être divisé en trois catégories: l'architecture WLAN/Cellulaire, l'architecture ad-hoc, et l'architecture hybride [2]. Si les infrastructures constituant les réseaux sont de type passerelles cellulaires ou WLAN ou encore des points d'accès WIMAX, le réseau est considéré comme cellulaire/WLAN pure. Par contre si aucune

infrastructure n'intervient durant les échanges entre les véhicules, il s'agit d'une architecture ad-hoc. Si les véhicules ont le choix d'utiliser une infrastructure disponible ou de communiquer directement de façon ad-hoc, on parle alors d'une architecture hybride.

Dans cette section, nous présentons quelques-unes des caractéristiques des VANETs : Dans un premier temps, nous présentons caractéristiques des canaux, dans un second temps, nous présentons les équipements qui rendent intelligents les véhicules et enfin, nous présenterons les relations entre les véhicules et les infrastructures.

2.1.1 Caractéristiques des canaux

Aux États-Unis en 1999, la commission fédérale de communication (Federal Communications Commission: FCC) avait alloué un bloc de spectre entre 5.850 et 5.925Ghz pour la communication véhiculaire (VC). Au Japon, une bande passante de 700 MHz est utilisée. Pendant ce temps, en Europe, des bandes de fréquences similaires étaient attribuées. Pour les mêmes raisons, la FCC a attribué une bande passante de 75MHz pour les communications entre les véhicules. Ces communication sont connu sous le nom DSRC [3]. DSRC est base sur la technologie IEEE 802.11P qui est pressentit pour devenir le standard des communications entre véhicules [5]. Ce standard qui est spécifié pour les VANETs utilise un canal de 10MHz. La vitesse de transmission est considéré entre 3 et 27Mbps pour chaque canal [9]. Les véhicules envoient des informations périodiques à leurs voisins grâce à des trames beacon pour une fréquence de 10 messages par seconde et un rayon de transmission maximum de 150 mètres.

2.1.2 Les équipements de bord

Les équipements de bord sont installés dans les véhicules afin de les rendre intelligents et les permettre de communiquer [10, 11]. Il s'agit de :

- **L'enregistreur de données des événements (EDR)** enregistre tous les événements qui se sont produits dans l'environnement du véhicule pendant le voyage;
- **Le récepteur (GPS)** communique l'emplacement géographique, la vitesse, la direction et l'accélération véhicule à des intervalles de temps spécifiés;
- **Le dispositif informatique** est utilisé pour prendre des mesures appropriées en réponse aux messages reçus des autres nœuds;

- **Les radars et des capteurs** are sont utilisés pour détecter des obstacles dans l'environnement du véhicule;
- **L'antenne omnidirectionnelle** est utilisée pour l'accessibilité au canal sans fil;

2.1.3 Relation entre les véhicules et les infrastructures

Dans un système VANET, il ya certaines entités telles que les autorités de transport régionaux (Regional Transportation Authorities :RTAs), les autorités de réseaux (Network Authorities :NAs), les autorités de droits(Law Enforcement Authorities : LEAs), les infrastructure placées au bord de la route sont utilisés pour la gestion des pseudonymes, l'accès à Internet et à d'autres services [3, 12]. Dans ce système, le « RSU » fournit l'accès aux infrastructures et services réseaux. Ils sont gérés par des fournisseurs de services tiers.

Les communications Véhicule à véhicule (V2V) et véhicule à infrastructure (V2I) constituent les deux aspects de communication dans les VANETs.

Dans les communications véhicule à véhicule, les nœuds peuvent communiquer directement entre elles par des connexions ad-hoc ou indirectement en mode multi-saut. Quand un véhicule est confronté à une situation dangereuse, il communique avec les autres véhicules pour les avertir qu'ils devraient éviter la zone de danger, à l'aide des communications V2V. Les communications V2V sont réparties en deux types : "un-saut" et "multi-saut", selon la position de l'émetteur et du récepteur. Pour la transmissions des messages de sureté en broadcast, les véhicules peuvent utiliser les communications de type multi-saut, si le message n'est pas sensible, c'est-à-dire que ce n'est pas un message de sureté par contre, pour les messages sensibles, ce sont les communications à un saut qui sont privilégiées [13].

Les communications véhicule-à-infrastructure interviennent pour les échanges entre les véhicules et les infrastructures placées le long des rues. Ces communications ont pour principales but d'éviter les accidents de la circulation. Les infrastructures transmettent des informations pertinentes aux véhicules selon la situation et le lieu. Il peut s'agir d'informations sur les conditions routières à cet hauteur, ou encore le véhicule peut accéder à des services telles que la mise-à-jour de clé de sécurité ou encore à une connexion Internet [14].

2.2 Les applications

Le développement des véhicules intelligents a apporté de nouvelles possibilités d'application dans les VANETs. Ces applications peuvent être catégorisées en : Application de transport intelligent et en application de confort et de maintenance [2].

Les applications de transport intelligent regroupent les applications de sureté et les applications de transport efficace. La fonction principale des applications de sureté est d'aider les automobilistes à éviter les accidents [9]. Ces applications interviennent pour des situations d'urgence. Les applications de confort ont pour but de rendre le voyage agréable pour les usagers de la route [5]. Dans cette section, nous présentons les applications selon leur utilités telle que présenté plus haut.

Les applications de sureté permettent l'évitement des collisions, ce qui même à éviter les accidents de la circulation. Par exemple, si un accident se produit loin sur la route, les véhicules s'informeront les uns aux autres ainsi, ceux qui s'approchent du lieu de l'accident pourront ralentir ou même changer de voie. Ce type d'application permet aussi de réduire les longues files sur la route à la suite d'un accident [3]. Dans certaines intersections qui ne disposent pas de feux de circulation, une application d'avertissement d'intersection pourrait aider les usagers à prendre leurs dispositions à l'approche de cette intersection. Un consortium formé des gouvernements et des acteurs de l'industrie automobile avait présenté plusieurs applications de sureté [28]: Application d'avertissement de la violation des feux de circulations, application d'avertissement d'une courbe sur la route [29], application de freinage d'urgence, application d'avertissement de collision [30], application de d'avertissement de collision coopérative, application d'assistant d'aide au tournage à gauche, application d'avertissement de changement de voie, application d'avertissement à l'arrêt de mouvement. Il existe d'autres applications qui sont plus utiles pour la prévention, il s'agit des application de gestion du trafic, des applications de monitoring du trafic, application d'analyse des condition de la route [32].

Les applications de confort quand à elles ont pour but principal d'améliorer le confort des usagers des la route pendant leur voyages. Plusieurs applications sont exploitables dans ce cas: Les applications de jeux en ligne et en réseau, les application de partage de music et de vidéo, l'accès aux informations, l'accès à la messagerie web , les communications interactives, l'accès aux informations utiles tel que le restaurant le plus proche, la stations de service à proximité, les parking disponibles dans les environs, etc. Les applications de maintenances sont utiles pour les

automobilistes qui rencontrent des problèmes mécaniques et qui nécessitent une aide urgente. Ils pourraient de ce fait bénéficier d'une aide à distance grâce à ces applications de maintenance. [2, 6].

2.3 Les requis de sécurité

Il est primordial de discuter des requis que doit respecter un système pour son bon fonctionnement avant d'adresser les questions relatives à la sécurité de ce dernier. Lorsqu'un requis n'est pas respecté, ceci précent une faille de sécurité. Les requis que doit respecter un VANET ont été présenté dans [3, 6], il s'agit de: l'authentification, l'intégrité, la confidentialité, la non-répudiation, le contrôle d'accès, les contraintes de temps réels et la protection de la vie privée. La plupart de ces requis dérivent de principaux buts de sécurité de tous systèmes et d'autres sont propres aux VANETs. Dans la suite nous détaillons les différents requis précédemment cités.

2.3.1 L'authentification

Ce requis est l'un des principaux de tout système. Pour les VANETs, il très important de connaitre plusieurs informations sur le nœuds émetteur tel que son identifiant, son adresse, ses propriétés , sa position géographique. Il est donc important d'authentifier l'émetteur du message et le message qui circule sur le réseau. L'authentification a pour objectif principal de contrôler les niveaux d'autorisation du véhicule dans le réseau. Dans les VANETs, l'authentification peut aider à la prévention des attaques de Sybil en spécifiant un identifiants unique pour chaque véhicule. Grâce à cette technique , un véhicule ne pourra pas clamer d'avoir plusieurs identifiants et de faire croire qu'il s'agit de plusieurs véhicules et ainsi perpétrer une attaque sur le réseau [23].

Plusieurs types d'authentifications ont été présenté dans [33] :

- **L'authentification de l'ID**, C'est le fait pour un nœud d'être capable d'identifier les transmetteurs d'un message donné de façon unique. C'est par cette authentification que passe l'accès au réseau du véhicule émetteur.
- **L'authentification de la propriété,** elle aide à déterminer le type d'équipement qui est en communication. Il peut s'agir d'un autre véhicule, d'un « RSU » ou encore d'un autre équipement.

2.3.2 L'intégrité

Elle s'assure que le message n'est pas altéré entre l'émission et la réception. Le récepteur du message vérifie le message reçu. Il s'assure que l'identifiant de l'émetteur reste le même tout au long de la transaction, et que le message reçu est bien celui qui a été émis [34]. L'intégrité protège contre la destruction et l'altération du message pendant la transmission. Si un message corrompu est accepté, on considère qu'il y'a eu une violation de l'intégrité. Pour mettre en place l'intégrité, le système devrait prévenir les attaques contre l'altération des messages, car le contenu du message doit toujours être fiable [35].

Certain protocoles de sécurité utilisent la signature électronique pour se rassurer que le message n'a pas été altéré Durant la transaction. Ainsi, à l'arrivé du message, la signature est vérifiée pour juger de l'intégrité du message [36].

2.3.3 La confidentialité

Le cryptage des messages permet d'empêcher à des véhicules n'ayant pas les autorisations nécessaire de lire les messages qui ne leurs sont pas destines. Cette mesure permet de respecter la confidentialité des échanges [35, 37]. La confidentialité des messages dans les VANETs dépends de l'application et du scenario de communication. Par exemple les messages reliés à l'avertissement d'une situation d'urgence peuvent être lu par n'importe quel membre du réseau. Ce type de message n'a donc par besoin d'être crypté. Par contre pour une application de paiement en ligne, il est important que les messages soient cryptés pour ne pas divulguer des informations sensibles sur une carte de crédit par exemple. La confidentialité peut être mis en place en utilisant les clé public/privé pour le cryptages des message Durant la communication [3].

Dans les communications V2I, les « RSU » et le véhicule se partagent une clé de session après avoir effectué une authentification mutuelle. Ainsi tous les messages sont cryptés avec la clé de session et sont aussi attaché un code d'authentification du message(Message Authentication Code :MAC) pour l'authentification du message [33].

2.3.4 La non-répudiation

Ce requis permet d'empêcher une entité de nier d'avoir participer à une communication. Il permet de protéger le système contre le déni d'un nœud qui indique n'avoir pas participé à une communication alors qu'il l'a fait. La non-répudiation permet donc au récepteur de prouver qu'il

a reçu le message d'un tiers de communication. Ainsi, pour chaque message reçu, l'émetteur peut être clairement identifié [38] .

Le but général de la non-répudiation est de collecter, de maintenir et de rendre disponibles toutes les évidences à propos d'un évènement ou d'une action, afin de résoudre des disputes à propos d'une occurrence ou non d'une action. La non-répudiation dépend donc de l'authentification. Le système peut ainsi identifier l'auteur d'un message malveillant [23]

2.3.5 La disponibilité

Le réseau et les applications doivent rester disponibles même en présence de panne dans le réseau. Ce requis permet non-seulement de sécuriser le système mais rend aussi celui-ci tolérant aux fautes. Ainsi les ressources doivent rester disponible jusqu'à ce que la faute soit réparée [39]. Un protocole de routage adéquat est nécessaire pour atteindre tous les récepteurs d'un message envoyé. Certain messages doivent rester circonscrit à un moment ou à un endroit définie, pour ne pas induire en erreur les véhicules si l'information n'est plus pertinente [40].

Plusieurs applications nécessitent une réponse rapide de la part des capteurs ou du réseau ad-hoc, car le délai rendra le message obsolète. Ce qui peut causer des situations désastreuses. Il est donc primordiales que les ressources soient disponible en temps et lieu opportuns [20].

2.3.6 Le contrôle d'accès

Ce requis a pour rôle de déterminer les droits et les privilèges dans les réseaux. Certaines communications comme celle de la police ou d'autres autorités ne doivent pas être écoutés par les autres usagers. L'accès à certains services fournit par les infrastructures est réservé à une catégorie d'usagers. Il est donc primordial de mettre en place un système qui permet de définir toutes ces politiques d'accès pour garantir le contrôle d'accès dans le réseau [39].

2.4 Les menaces de sécurité

Comme chaque réseau classique, il existe plusieurs attaques de sécurités. Pour le cas des VANETs, il en existe encore plus. Le fait est que ces réseaux n'ont pas encore réellement été implémentés. Du coup, il est difficile de définir toutes les attaques pouvant y être perpétrés. Les chercheurs en plus de considérer les attaques des MANETs, ont imaginé d'autres attaques dont pourrait être encouru les VANETs. Dans cette section, nous présentons les différentes menaces

que peut encourir un VANET. Cette classification est faite en considérant des paramètres tels que : l'étendu de l'attaque, l'impact de l'attaque sur le réseau, les requis à respecter pour ce réseau, les solutions possibles pour protéger le réseau et le profil des attaquants éventuels [1-3, 5, 20, 36] Parmi les attaques, citons:

Le déni de service: Cette attaque peut être considérée comme la plus populaire dans les réseaux classique et elle peut aussi être perpétrée dans les VANETs. L'intérêt de ce type d'attaque est de rendre le réseau disfonctionnel. Ainsi donc le VANET ne sera plus disponible [20, 36]. Un attaquant peut mettre en place cet attaque en inondant le réseau, en insérant des informations non pertinentes dans le réseau [58]. Un farceur peut rendre le réseau indisponible pour la simple raison de prouver qu'il en est capable. L'étendu de ce type d'attaque est généralement large, ce qui signifie que c'est une attaque qui concernera un grand nombre de nœuds. Ainsi donc, c'est une attaque qui peut s'étendre dans une zone géographique très large à travers plusieurs nœuds par des communications multi-sauts. De plus, l'impact de ce type d'attaques se reflète par le fait que l'attaque peut être détectée, mais il sera difficile de la corriger [51, 59]. Les requis concernés par ce type d'attaques sont : l'intégrité des données, certains messages pourraient être altérés si les lignes de communication ne sont pas disponibles. Il est évident que le requis de disponibilité sera aussi mis en cause. Si le réseau est indisponible, il y'a de forte chance que les donnés ne soient pas disponibles pour les applications. Les contraintes de temps réels ne peuvent non plus être respectées dans ces conditions. Ahmed et al. [60] ont présenté une solution dans laquelle les équipements de bords sont utilisés pour prendre une décision afin de dissuader les éventuels attaquants. Dans le cas d'une attaque de déni de service, le processeur du système suggère aux équipements de bords de changer de canaux de communication, ou d'utiliser une technique de saut de fréquence. Ce type d'attaque peut être perpétrer par n'importe quelle type d'attaquant, il va de soit qu'un membre du réseau a plus de chance de réussir son attaque, par rapport à un autre qui ne fait pas partie du réseau.

L'écoute des messages: Cette attaque consiste pour un attaquant de se positionner à une position dans un véhicule (en arrêt ou en mouvement) ou de se présenter comme un faux « RSU » [61]. Le but de cet attaque est d'accéder à des informations concernant d'autres nœuds et ceci de façon illégal. Le requis mis en cause dans ce type d'attaque est celui de la confidentialité. Le cryptage des message est l'une des solutions préconisée pour y faire face [62].

L'usurpation d'identité: Ce type d'attaque consiste à prendre l'identité de quelqu'un d'autre et de faire croire que vous êtes cette personne [39, 61]. Ainsi un adversaire peut perpétrer des actions malicieuses en incorporant dans les messages l'identifiant d'un autre nœud. Lorsque les autorités recherchent le coupable de l'action malicieuse perpétrée, ils iront chercher la personne dont l'identifiant a été dérobé. Pendant ce temps, le vrai coupable sera dans la nature. C'est une attaque qui fonctionne pour une communication à un saut car l'attaquant attaque directement sa cible sans passer par des nœuds intermédiaires [63]. Ce type d'attaque est difficile à détecter et même difficile à corriger, surtout si la cible est isolée. Les requis qui sont mis en cause dans ce type d'attaque sont : la non-répudiation, si l'identifiant est erroné il est presqu'impossible de retrouver le nœud réellement fautif. La confidentialité et le contrôle d'accès sont aussi en cause dans ce type d'attaques. Car le nœud malicieux peut recevoir des informations en lieu et place du propriétaire de l'identifiant volé. Ce derniers peut aussi accéder à des informations et des services qui étaient réservés pour le propriétaire de l'identifiant. Cette attaque porte finalement accès à la vie privé de l'usager propriétaire de l'identifiant. Les signatures numériques et les système de certificats permettent de prévenir ce type d'attaque [64]. La signature des messages permet aussi de prévenir l'attaque d'usurpation d'identité. Ainsi l'adversaire pourra recevoir le message mais sera incapable de le lire. Ce type d'attaque est facile à réaliser par des nœuds qui sont déjà membre du réseau [65]. L'adversaire qui perpétue ce type d'attaque agit de façon rationnelle.

Altération/falsification des messages: La falsification des messages consiste à changer les informations contenues dans un message lors de son passage à travers un nœud. On parle ainsi d'attaque d'altération lorsque le contenu du message est altéré par un adversaire [66, 67]. Un nœud malicieux peut ainsi changer le contenue ou même le type du message en faisant par exemple croire qu'il y'a un accident alors que ce n'est pas le cas. Ce type d'attaque est souvent perpétrer par un nœud intermédiaire par lequel le message transite pour retrouver son récepteur. C'est donc une attaque qui est perpétré lors de communications multi-sauts. Par contre ce type d'attaque peut être détecté si le message transite par d'autres nœuds dans le réseau. Dans ce cas il est possible de déterminer que l'information provenant de ce nœud est différent de celle provenant d'autres nœuds du réseau. Mais si le nœud adversaire est le seul par lequel le message transite, il sera difficile de détecter et d'éviter l'attaque [16]. Cette attaque peut être étendue si plusieurs nœuds reçoivent l'information provenant seulement de l'adversaire. Si un seul nœud reçoit cette information alors l'attaque est limitée à ce seul nœud. Dans ce type d'attaque, le

requis concerné est l'intégrité, car le message étant altéré, son intégrité n'est plus garantie. La vérification des messages peut être utilisée pour prévenir ce type d'attaque [68].

Délai/Suppression des messages: C'est le fait pour un adversaire de conserver le message pendant une certain durée avant le retransmettre [52, 69]. Cette situation a pour effet de créer un délai sur la transmission du message. Dans le pire des cas, l'adversaire peut tout simplement détruire le message et ne pas le transmettre. Le fait de créer un délai au transfert du message occasionne de graves conséquences; surtout s'il s'agit d'application exigent du temps réel [23]. Par exemple un message à propos de l'avertissement d'un accident qui est supprimée causera l'aggravation de l'accident car les véhicules n'ayant pas été informé d'un accident iront s'engouffrer ce qui fera grandir l'ampleur de l'accident. D'autre part, un adversaire peut publier un ancien message concernant un accident. Cette situation aura pour conséquence de faire croire aux autres véhicules qu'il y'a réellement un accident et ainsi causer des situations malencontreuses des véhicules qui agiront comme s'il y'avait un accident [64]. Cette attaque est similaire de celle précédemment présentée dans la mesure ou le message est intercepté par un véhicule intermédiaire et utilisé à d'autres fins. Mais dans ce cas, ce n'est pas l'intégrité du message qui est en cause mais c'est le message lui-même. Dans le cadre des applications VANETs qui sont généralement contraintes au temps réel, cette situation n'est pas acceptable [19]. C'est une attaque difficilement détectable et corrigible. Le principal requis en cause ici est celui du respect du temps réel et de la disponibilité [70].

Attaque sur le matériel: Cette attaque concerne les équipements matériels. L'adversaire dans ce cas agit physiquement sur les équipements de façon à les rendre dysfonctionnels. [20, 71]. Les équipements visés ici sont : les équipements des communications telles que les antennes ou les interfaces de communication, les équipements de calcul tel que l'ordinateur de bord ou encore les équipements de collecte d'information telle que les capteurs, les radars ou encore les récepteurs GPS. Le requis en cause dans ce cas est la disponibilité, les équipements n'étant pas fonctionnelles, il est impossible d'accéder aux ressources, aux services ou encore aux informations [72]. Une des solutions proposée pour éviter ce type d'attaque repose sur la technique de l'utilisation de la plate-forme TPM(Trusted Platform Module) [73].

Il est toujours possible de trouver d'autres attaques, la liste que nous avons présentons plus haut n'est pas exhaustive. Elle a pour but de présenter les principales attaques auxquelles sont soumises les VANETs, à celles-ci peuvent dériver de nouvelles autres attaques.

2.5 Solutions pour la sécurisation des VANETs

Dans la littérature, plusieurs solutions ont été proposées pour adresser le problème de la sécurité dans les VANETs. Dans cette section, nous présentons certaines solutions et architectures.

Dans [43] Raya et al. proposent une analyse détaillée des menaces qu'encourent les VANETs et proposent une architecture de sécurité. Ils ont présenté un ensemble de protocoles de sécurité de vie privée et la robustesse de ces protocoles. Après la présentation de certains requis de sécurité et des profils des attaquants, ils ont proposé leur propre solution. Dans un premier ils ont présenté les signatures numériques comme un block. Dans cette section, l'emphase a été mise dans le fait que dans les VANETs, les message de sureté nécessite une authentification et leur préférence pour la sécurisation des message par signature numérique.

Dans un second temps ils ont présenté une façon de sécuriser les messages. Avant qu'un véhicule n'envoie un message de sureté, il le signe par une clé privée et inclure une autorité de certification (CA). Après la présentation de leur méthode de sécurisation, ils ont proposé un dispositif inviolable pour sécuriser physiquement des informations sécrètes, telles que les clés privées. Ce dispositif pourrait également signer les messages sortants.

Troisièmement, ils ont propose une façon de gérer les clés. En d'autres termes, ils ont adressé la question de la distribution des clés de certification et de révocation. À cette fin, ils ont identifié deux composants relatifs à la cryptographie: l'identité électronique et les pairs de clés anonymes qui sont utilisées pour la question de la confidentialité. Cette clé sera conservée et distribuée par les autorités gouvernementales de transport ou par les constructeurs automobiles. La clé doit être certifiée par une autorité de certification. La clé sera révoquée dans le cas d'une observation d'une activité compromettante. Dans le but d'assurer la vie privée des usagers, les auteurs proposent l'utilisation de clé publique anonymes. Pour l'authentification d'établissement de session, il est proposé d'utiliser des primitives cryptographiques symétriques. Pour prévenir les attaques de déni de service, il est proposé de commuter entre différents canaux ou même des technologies de communication. Pour éviter les attaques de divulgation d'information erronées, il est propose de faire une vérification des données reçues d'un émetteur en les comparant avec des informations provenant d'autres sources. L'anonymat des usagers est assuré par un algorithme de changement de clé qui s'adapte à la vitesse du véhicule et prend en compte la corrélation de la clé par l'adversaire.

Dans [33], Frank Karl et al. ont suggéré la méthode SECA(the Security-Requirements Engineering using Cluster Analysis). C'est une approche qui permet l'analyse d'un grand nombre d'applications en sélectionnant une représentation typique qui couvre les requis du cluster d'application, ensuite, ils développent une solution de sécurisation pour ce sous-ensemble d'application (fig. 1). Ainsi, dans un premier temps, ils collectent une liste d'application qui comprend les différents cas d'utilisation possibles. Dans un second temps, ils font une analyse préliminaire des caractéristiques des applications précédemment sélectionnées et les requis de sécurités de toutes les applications en question. Une fois l'analyse effectuée, ils regroupent les applications similaires en utilisant un cluster d'analyse. En quatrième lieu, ils appliquent des cas d'utilisation d'attaques à un sous-ensemble d'applications représentatives de chaque cluster et les analysent plus en détails. À partir de cette étape, ils sont capables de déterminer un ensemble de mécanisme de sécurité à appliquer à ce sous ensemble d'application pour les prévenir d'éventuelles attaques. En fin de compte, ils déterminent les mécanismes de sécurité pour tous les sous-ensembles d'applications formés.

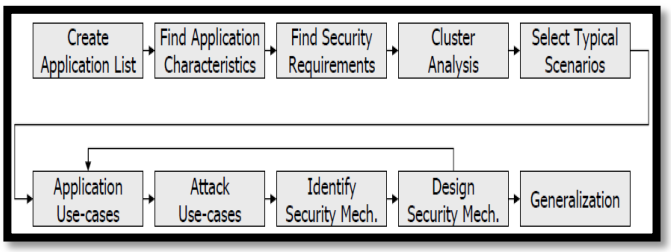

Figure 2.1 : Les étapres du processus « SECA »

Klaus et al. ont propose dans [40] une architecture de sécurité pour les VANETs (SAV), cette architecture est présenté à la figure 2-2. Le modèle de communication de cette architecture est base sur le fait qu'il existe deux types de communications: la communication des messages passifs tels que les messages beacons qui sont envoyés de façon périodique et la communication des messages actifs qui sont envoyé lorsqu'un évènement a lieu et qu'un avertissement doit être envoyé aux véhicules voisins. L'architecture de sécurité qu'ils proposent pour les VANETs se divise en trois couches :

(1) La couche basse qui inclut les éléments de sécurité de base. Dans cette couche, il est suggéré d'utiliser une infrastructure centralisée à clé publique(public key Infrastructure :PKI)

avec un tiers de confiance (Trusted Third Party : TTP). Ceci permettra d'assurer la vie privée des usagers.

(2) La couche de sécurité à un saut est une couche dans laquelle l'on peut observer la manière dont les trames beacons sont sécurisés. Le récepteur des trames beacon à la possibilité de vérifier l'intégrité de ces derniers, en même temps que l'identifiant de l'émetteur comme participant valide dans le VANET. Ceci est possible car chaque nœud est obligé de signer numériquement ses messages. La vérification est faite en utilisant la certification CertS. Les deux véhicules qui veulent communiquer doivent s'assurer que le CertS est authentique et les deux sont fiables avant le début de la communication.

(3) La couche multi-saut, elle inclut toutes les autres applications et services utilises dans les VANETs. Cette couche est applicable pour les signaux d'alarme, les applications d'avertissement et les services de valeurs ajoutés dans les VANETs. À cause de l'importance de vérifier certaines informations envoyées par le nœud qui aimeraient entrer en communication, le nœud récepteur peut utiliser la méthode de camouflage spatiale pour vérifier la position géographique du nœud.

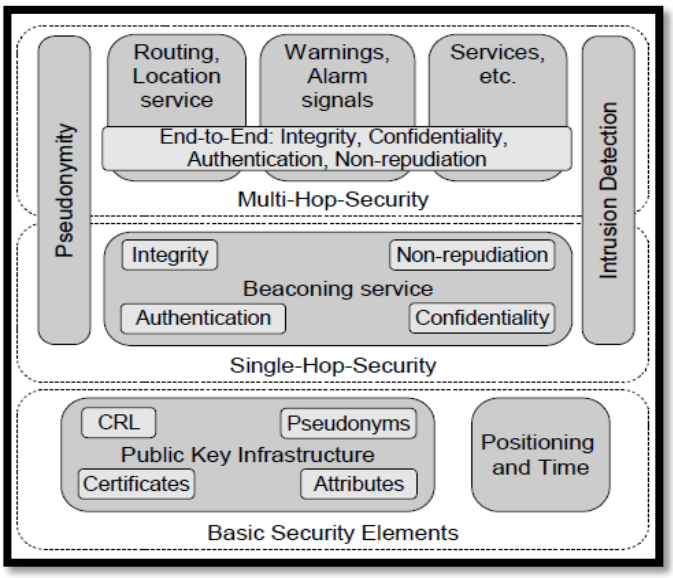

Figure 2.2:Architecture de sécurité

Dans [74] Dhurandher et al. présentent la sécurisation des véhicules par les algorithmes de réputation et de vérification (Vehicular Security through reputation and Plausibility Check Algorithm :VSRP). Pour déployer la sécurité dans les VANETs, leurs algorithmes prennent en considération trois types d'évènements : les embouteillages, les accidents et les applications de freinage. L'algorithme utilise un système base sur la réputation des capteurs, non seulement pour

détecter mais aussi pour isoler les nœuds malicieux présents dans le réseau. Cet algorithme permet aussi de gérer les problèmes lies à l'agrégation et la suppression des données.

Cet algorithme exploite une approche orienté évènement. Trois types d'évènements sont répertoriés: 1) un-saut, 2) multi-saut, 3) intention malicieuse. Le protocole distingue deux type de paquets pour les messages : (1) les parquets de données, (2) les parquets de requêtes des voisins (neighborreq packet), (3) les paquets de réponse des voisins (neighborrep packet). Pour conserver les informations, chaque nœud maintien cinq tables : la table des voisins, la table de confiance, la table "reqseen", qui est utilise pour maintenir les informations à propos d'un nœud qui a envoyé une requête, la table des données qui est utilisé pour maintenir les informations à propos des paquets de données, et enfin la table temporaire qui est utilisée pour temporairement utilisé pour stocker les information collectées par un nœud. Dans le cas des accidents et des embouteillages, l'algorithme proposé est divisé en quatre phases : (1) la découverte du réseau, (2) la distribution des données, (3) la prise de décision, (4) la mise-à-jour des valeurs de confiance et l'observation des voisins.

Dans [37], Phillipe Golle et al. ont proposé une approche générale pour évaluer la validité des données dans le VANET. Dans leur approche, le nœud cherche les différentes explications possibles à propos des données qu'il a collecté; basé sur la supposition qu'un nœud malicieux peur être présent. Si l'explication est consistante par rapport au modèle du VANET, les données sont acceptées et enregistrées et acceptés par le nœud avec un score d'explication élevé. Leur techniques pour évaluer et classer les nœuds dépend de deux hypothèses: (1) les nœuds ont une habilité pour s'échanger les informations les uns avec les autres, (2) un argument de parcimonie reflète fidèlement un comportement contradictoire dans le VANET. Pour mener à bien leur but, ils ont proposes une technique général base sur le comportement des capteurs. Cette technique leur permet de détecter les informations incorrectes sur l'identité du nœud ou des nœuds émetteurs de ces informations incorrectes avec une probabilité élevée. Les succès de cette approche est base sur le fait que chaque nœud maintien un modèle du VANET contenant toutes les informations que ce nœud possède à propos du VANET en question. Lorsqu'il y'a une inconsistance des données, le nœud essaiera de comprendre pourquoi cette situation survient-t'elle? Cette tâche est réalisée en exploitant un algorithme heuristique qui a été implémenté par les auteurs pour gérer le problème d'inconsistance des données. L'une des attaques dans les VANETs pourrait être l'attaque de sybil pour laquelle, un nœud peut utiliser des identifiants

virtuels pour prétendre qu'il s'agit de plusieurs nœuds physiques. Les auteurs utilisent le concept de « distinguishability ability » pour permettre aux nœuds honnêtes de déterminer la présence physique d'un autre nœud. Ils considèrent les cas ou le nœud peut utiliser ses équipements embarqué tel que la camera, les capteurs physique, etc. pour confirmer la présence physique d'un autre nœud. Pour détecter la présence physique des nœuds éloignés, ils font tout simplement confiance aux nœuds intermédiaires pour déterminer la présence physique. Ce choix est fait avec l'hypothèse que les communications sont authentifiées.

Plusieurs approches ont été définies pour la sécurisation des VANETs, certaines sont générales et d'autres sont spécifiques. Le challenges demeure cependant de proposer une méthode qui permette de protéger le VANET dans son ensemble et en considérant toutes les applications.

2.6 Conclusion

Dans ce chapitre, nous avons brossé un état de l'art de la sécurité dans les VANETs. Après avoir présenté l'architecture et les caractéristiques des VANETs, dans lesquelles nous avons présenté les différentes bande de fréquences adoptées dans le monde à propos des communications, et des canaux utilisés pours ces communications, nous parlé des relations entre les véhicules et entre les véhicules et les infrastructures. Nous avons ensuite présenté les challenges dans les VANETs, dans cette partie, nous avons invoqué les contraintes temps réel, la grande largeur des VANETs, la très grande mobilité des nœuds dans ces réseaux. Nous avons ensuite vu qu'il existe plusieurs applications qui sont implémentées dans les VANETs, nous avons surtout pointé les application de sureté qui permettent surtout d'éviter les accidents et les applications de confort et de maintenance qui favorisent le bien être des usagers de la route pendant leur voyages. Nous nous sommes aussi attarder sur les requis que doit respecter un réseau VANET, nous en avons présenté certains comme l'intégrité, la confidentialité, l'authentification la non-répudiation, etc. À la suite de cela, nous avons présenté les menaces encourues par les VANETs, nous avons vu qu'il y'en avait plusieurs, mais nous en avons cité quelques une telles que les dénis de service, l'usurpation d'identité, la suppression, l'altération et les délais sur les messages, nous avons aussi vu que certaines attaques pouvait cibler les équipements physiques embarqué dans le véhicule. Enfin, nous avons présenté quelques solutions proposées dans la littérature. Nous avons surtout constaté que toutes les solutions proposées résolvent partiellement le problème de sécurité dans les VANETs. De ce fait le challenge

demeure de proposer une solution qui prenne en charge la sécurité globale des VANETs, en terme d'application et de réseau sous-jacent.

CHAPITRE 3

LE CONCEPT DE RÉPUTATION

Le dictionnaire Larousse définit le concept de réputation comme étant l'opinion favorable ou défavorable du public à propos d'une personne ou d'une chose. En effet cette définition peut être considérée selon chaque contexte particulier. La réputation a été l'objet d'étude dans plusieurs domaines tels que l'économie, les sciences sociales, l'informatique [96]. Certains sites de commerce électroniques ou de ventes aux enchères en ligne tel qu'eBay et Amazon respectivement sont des exemples où les systèmes de réputation ont été implémentés avec succès. Le concept de réputation peut aussi très bien sied aux réseaux informatiques auto-organisés tel que les réseaux pair à pair (P2P), les réseaux de capteurs et les réseaux ad-hoc mobiles [97]. Ce concept trouve son intérêt dans le fait qu'il permet de doter les systèmes des moyens efficaces permettant aux acteurs de décider avec qui communiquer; dans des environnements où les acteurs n'ont pas une connaissance préalable les uns avec les autres. Ainsi une relation de confiance peut être établie et faciliter les échanges. Les systèmes de réputation appliqués dans un environnement de réseaux mobiles peuvent permettre d'éviter certaines attaques visant ces réseaux. Car la connaissance préalable de certaines informations sur le nœud émetteur, peuvent aider le nœud récepteur à prendre la bonne décision avant d'accepter ou non de communiquer avec ce dernier. Les systèmes de réputation ont fait leurs preuves dans plusieurs applications populaires. Le célèbre moteur de recherche Google par exemple utilise un algorithme qui implémente la réputation pour définir l'ordre d'affichage des pages web selon une recherche par mots-clés effectuée par un usager. Dans son système de sécurisation des entités électroniques, McAfee s'est doté d'un système de réputation performant pour évaluer les entités potentiellement dangereuses ou non. De plus en plus de chercheurs dans le domaine de la sécurisation des réseaux mobiles s'intéressent à la sécurisation de ces réseaux par des méthodes de réputation [92, 97-101].

Nous présenterons dans une première section, les systèmes de réputation dans leur généralité, ensuite nous aborderons le cas des réseaux informatiques auto-organisés.

3.1 Généralités sur les systèmes de réputation

La prise de décision est une tâche difficile quelque soit le domaine dans lequel l'on agit; que ce soit dans les sciences sociales pour les relations entre les humains, dans la médecine pour la pause de diagnostic ou encore en mathématique pour l'évaluation d'instruments financiers, les acteurs font très souvent appel aux systèmes de réputation pour l'évaluation de la situation et la prise de décision [102].

Selon l'encyclopédie en ligne, Wikipedia [103], *« les systèmes de réputation sont des systèmes qui calculent et publient des scores sur un ensemble d'objets (par exemple des pourvoyeurs de services, les services, les biens ou d'autres entités) d'une communauté ou d'un domaine basé sur une collection des opinions que les autres entités ont collecté à propos de ces objets. L'opinion est ainsi soumis à un centre de réputation qui permet de calculer les scores de réputation grâce à des algorithmes et ce de façon dynamique »*. Nous pouvons ajouter à cette définition que dans certains cas l'opinion est aussi forgée grâce à l'expérience et aux observations propres de l'entité elle-même. L'éclosion des transactions et des communications web, notamment avec l'avènement du commerce électronique, avec les échanges de fichiers et d'information entre les internautes en P2P, avec les réseaux sociaux. Les fournisseurs et les consommateurs de biens et de services sont de plus en plus soucieux de la fiabilité des communications ou des entités avec lesquelles ils entrent en contact ou avec lesquelles ils sont en affaire. De fait le calcul de la réputation des tiers prenant part aux transactions prend tout son intérêt. Cette recherche de fiabilité par des outils de réputation donne naissance à divers modèles de « confiance » tiers, des plus légers tel que les votes communautaires au plus lourds telles que les autorités de certification aux programmes de labellisation [102]. Pour ce qui est du vote communautaire, les entités de la communauté utilisent les scores de réputation pour prendre des décisions, par exemple une décision peut reposer sur le choix d'un achat ou non d'un service ou d'un bien spécifique. Un objet possédant une meilleure réputation attirera l'attention par rapport à un objet à faible score de réputation. Il est donc intéressant pour chaque objet d'avoir un meilleur score de réputation. De même, un fournisseur de service réputé digne de confiance aura plus de facilité à trouver des clients par rapport à un fournisseur inconnu ou ayant une mauvaise réputation.

Le fait que l'opinion collective d'une communauté détermine le score de réputation d'un objet implique que les systèmes de réputation représentent une forme de sanction ou de gain à la

collaboration. Un bas score représente une sanction négative relative à la collaboration d'un objet qui a donné un faible rendement. De la même façon, un score de réputation élevé indique que l'objet a donné un meilleur rendement par rapport aux observations des membres de la communauté. Par contre, il est possible qu'un score de réputation élevé détenu par un objet décroisse très rapidement si l'objet en question cesse de fournir un rendement satisfaisant. De la même façon, il est possible pour un objet avec un mauvais score de remonter son score, si ce dernier commence à fournir un service satisfaisant aux yeux de la communauté.

Les systèmes de réputation peuvent être comparés aux systèmes de recommandation et aux systèmes de filtrages collaboratifs. Contrairement à ces deux derniers, le système de réputation produit un score basé sur une notation explicite de la communauté alors que les systèmes de recommandation se basent sur des évènements externes pour générer des recommandations commerciales. D'après [104], le rôle des systèmes de réputation est d'établir la fiabilité. Les systèmes de réputation sont très utilisés dans les grandes communautés d'utilisateurs en ligne dans lesquelles les utilisateurs ont souvent l'opportunité de discuter les uns avec les autres sans aucune connaissance préalable. Des sites web tels que Youtube.com ou Flickr.com où les utilisateurs peuvent poster et générer des contenus en sont quelques exemples. Dans ce cas, il est judicieux de se baser sur l'expérience d'autres utilisateurs avant d'entrer en communication avec un tiers. Les systèmes de réputation peuvent aussi bien être couplés à des systèmes de récompense de façon à ce que les objets ayant un meilleur score de réputation bénéficient des privilèges dont les objets avec des mauvaises notes de réputation ne peuvent prétendre.

3.1.1 Intérêt de la réputation

De par sa capacité à être exploité dans les domaines divers, le concept de réputation présente un intérêt primordial pour l'analyse des comportements des entités dans un environnement donné. Dans les sciences sociales, la réputation permet l'étude de comportement des êtres humains dans un milieu social [105]. En économie, la réputation sert plutôt à l'analyse et à la prédiction des tendances économiques en tenant compte des réalités présentes et passées. En informatique, le concept de réputation est utilisé aussi bien dans le domaine de l'intelligence artificielle, du commerce électronique ou encore dans les réseaux auto-organisés (Réseau Ad-hoc, Réseaux de capteurs, Réseaux Mobiles, etc.) [96]. Pour ce dernier cas, il permet de garantir la

fiabilité des nœuds en communication. Il sert aussi de mesure de comportement des différents nœuds quant à leur collaboration dans la bonne marche du réseau.

3.1.2 Architecture d'un système de réputation

Un système de réputation fiable et efficace doit avoir certaines caractéristiques. La caractéristique fondamentale de ce dernier est la capacité de prédire un évènement futur en se basant sur des observations d'évènements passés [96, 106, 107]. Il est vrai que des cas d'exception peuvent être rencontrés si un nœud du réseau se comporte différemment dans le passé et dans le futur; mais ce type de comportement est particulier. On considère donc que les observations du comportement passé sont un indicatif clé du comportement futur d'un acteur. Sonja et Leboudec [96] ont soulevé plusieurs questions auxquelles il faut répondre pour concevoir un système de réputation fiable:

- Comment se fait la conservation des informations?
- À propos de qui les informations sont-elles conservées?
- Où se fait la conservation des informations collectées?
- Pour combien de temps se fait la conservation des informations?
- Quand-est-ce que ces informations sont-elles ajoutées dans le système?
- Comment sont considérées les informations provenant d'autres nœuds?
- Comment sont-elles intégrées au système de réputation?
- Quelle considération est-elle faite de ces informations au fil du temps?
- Quel évènement provoque le changement de ces informations?

En d'autres termes, le système de réputation peut être considéré comme un ensemble constitué d'un processus d'observation des comportements du voisinage, d'un processus de stockage des observations précédemment réalisées, d'un processus de traitement de ces informations et enfin d'un processus de prise de décision au vue des résultats des traitements effectués. Un système de réputation fiable est un système de réputation pour lequel le comportement du nœud est exemplaire. Il reste à déterminer quels critères doivent remplir un nœud pour être considéré comme étant exemplaire.

3.1.3 Questions sur la construction d'un système de réputation

Pour permettre aux concepteurs d'améliorer et de peaufiner leur système de réputation les auteurs de [96] ont soulevé une seconde série de questions :

- Quel est l'impact que peut avoir un nœud potentiellement dangereux sur un nœud honnête?
- Quel genre d'informations peut être envoyé à d'autres nœuds pour mettre en place un système de réputation efficace?
- Quelle stratégie un attaquant peut-il mettre en place pour corrompre un système de réputation de façon à mieux mentir?
- Comment est-ce qu'un système de réputation peut-il venir à bout des faux positifs ou négatifs?
- Quel impact des informations incomplètes peuvent-elles avoir sur un système de réputation? Par exemple pour les réseaux auto-organisés où le nœud n'a qu'une vision partielle du système.
- Quel est l'impact d'une mauvaise observation? (par exemple différencier une attaque de suppression de paquets et une coupure de la connectivité ou un problème de congestion dans un réseau sans fil)
- Pourquoi est-ce que les nœuds devraient-ils accepter de participer dans un système de réputation ? Existe-t-il un moyen d'encouragement à participer/coopérer et de contribuer dans le système de réputation et de le faire honnêtement?
- Dans quel mesure est ce que le système de réputation est-il fiable et efficace?
- Quelle est la pertinence des données enregistrées qui représentent le comportement du nœud dans le passé?

Si les deux séries de questions soulevées ci-dessus ont été répondues correctement, le système de réputation peut être considéré comme efficace. Les agents pourront donc s'y fier pour prendre des décisions éclairées.

3.1.4 Le calcul du score de réputation

Abul-Ranman et Hailes [108] proposent une méthode permettant de calculer le score de réputation. En effet ils proposent un système qui divise le score de réputation en intervalle. Ainsi,

le degré de confiance d'un agent pour un autre peut prendre quatre valeurs: très digne de confiance, digne de confiance, peu digne de confiance et absolument pas digne de confiance. Les témoignages provenant d'autres agents sont considérés avec un poids. Ce système a pour principal inconvénient le problème d'initialisation. Car un nouveau venu dans le réseau ne sait pas forcément à quel agent il doit se fier.

Josang [100] propose un modèle "d'opinion" dont le principe est d'avoir un quadruplet (*b, d, u,a*) qui exprime la croyance qu'un client *p* a en une déclaration binaire concernant un fournisseur de service (*FS*). Il considère de fait deux états: *FS* est digne de confiance ou alors *FS* n'est pas digne de confiance. Par contre il n'y a aucune certitude quant à la véracité de cette déclaration. Un agent fait donc preuve d'une opinion à propos de la déclaration en question. Cela se traduit par des degrés de conviction ou de méfiance, un dernier paramètre est utilisé pour caractériser l'incertitude. Les paramètres *b, d,* et *u* représentent respectivement la conviction "belief", la méfiance "disbelief" et l'incertitude "uncertainty", avec *b, d, u* appartenant à [0, 1]| *b* + *d*+ *u* =1. Cette égalité représente le fait que la conviction d'une personne croît en même temps que sa méfiance diminue, c'est-à-dire qu'une personne sûre de l'affirmation d'une déclaration n'est pas méfiante à propos de cette déclaration. Le paramètre *u* a pour rôle de nuancer les paramètres *b* et *d* dans la mesure où une entité peut ne pas être certaine d'une affirmation encore moins de la négation de celle-ci. *a* est un paramètre qui détermine le degré d'incertitude et contribue au calcul du score de réputation. En ayant pour opinion comme "*FS* est digne de confiance", la réputation de *FS* sera: $r = b + u \times a$. Dans le cas où "*FS* n'est pas digne de confiance", la réputation de *FS* sera : $r = d + u \times a$.

En considérant deux opinions tel que $w_1 = (b_1, d_1, u_1, a_1)$ *et* $w_2 = (b_2, d_2, u_2, a_2)$ à propos d'une même déclaration, on peut obtenir leur somme (c'est-à-dire une moyenne des deux opinions) $\overline{w}$= ($\bar{b}$, $\bar{d}$, $\bar{u}$, $\bar{a}$) comme suit:

$$\begin{cases} \bar{b} = (b1u2 + b2u1)/k \\ \bar{d} = (d1u2 + d2u1)/k \\ \bar{u} = (u1u2)/k \\ \bar{a} = (a2u1 + a1u2 - (a1 + a2)u1u2/(u1 + u2 - 2u1u2) \end{cases}$$

où $k = u1 + u2 - u1u2$ et $u , u2$ n'appartenant pas [0, 1]. Lorsqu'un agent p recommande un autre agent FS avec l'opinion $w_1 = (b_1, d_1, u_1, a_1)$ et que l'opinion de FS à propos d'une déclaration x

est $w_2 = (b_2, d_2, u_2, a_2)$, l'opinion de *p* à propos de x via la recommandation de *FS* est $w_R = (b_R, d_R, u_R, a_R)$ telle que:

$$\begin{cases} b_R = b_1 b_2 \\ d_R = b_1 d_2 \\ u_R = d_1 + u_1 + b_1 u_2 \\ a_R = a_2 \end{cases}$$

L'auteur explique cependant que certaines situations ne peuvent être complètement analysées sans ignorer certains témoignages. En effet, un tel réseau peut être vu comme un graphe orienté où les nœuds sont les agents et les arcs les recommandations. Lorsque deux chemins sont possibles, il faut choisir un unique chemin à prendre en compte, ce qui revient à abandonner certains témoignages. De plus, ce système n'est pas intuitif comme peut l'être une méthode de calcul de réputation additive, et prendre deux témoignages différents en compte est déjà complexe.

Ismail et Josang [109] proposent la béta-réputation, qui est un exemple de système bayésien. Ce système fait la supposition selon laquelle le comportement d'un agent suit une loi de probabilité beta de paramètre *a* et *b* inconnus.

3.1.5 Attaques ciblant les systèmes de réputation

Les systèmes de réputation sont sensibles aux attaques d'agents malveillants qui tentent par tous les moyens possibles de tirer profit des vulnérabilités de ces systèmes. Il existe dans la littérature de nombreux travaux qui adressent les questions liées à ce sujet [3, 16, 97, 110-113]. En plus des attaques portant sur les mécanismes internes des systèmes de réputation, d'autres essayent d'attaquer directement le réseau sous-jacent en injectant des informations erronées ou dangereuses ou encore en rendant tout simplement le réseau non-fonctionnel par des attaques de sybil ou de déni de service. Dans cette section, nous présentons quelques-uns des travaux qui abordent la problématique des attaques perpétrées sur les systèmes de réputation et les réseaux sous-jacents.

Carrara et Hogben [3] présentent de nombreuses attaques ciblant les mécanismes inhérents aux systèmes de réputation. Certaines ont une portée globale tandis que d'autres sont locales. Pour l'attaque de Sybil [110], un attaquant revendique plusieurs identités dans le système, ce qui lui permet de contrôler multiples nœuds, augmentant ainsi son influence sur le réseau – il peut

poster de nombreux témoignages fallacieux. L'utilisation d'une autorité de démarrage, demandant un coût avant de permettre l'entrée d'un agent dans le système, diminue le risque des attaques de Sybil. Cela peut se faire avec des puzzles calculatoires comme ceux présentés par Borisov [114]. Plusieurs attaquants peuvent également former une collusion. C'est-à-dire qu'ils mettent en commun leurs ressources et connaissances afin d'obtenir encore plus d'informations sur un autre agent ou de modifier la réputation d'un fournisseur de service.

L'attaque par blanchiment de réputation, est une attaque qui permet à un agent de réinitialiser son score de réputation lorsqu'il le juge trop faible. Un attaquant peut aussi vouloir filtrer l'ensemble des témoignages concernant un fournisseur pour augmenter la proportion de témoignages favorables et ainsi augmenter son score de réputation. Si un attaquant veut modifier la réputation d'un fournisseur de service – en termes d'amélioration ou de diminution –, il peut utiliser la technique du bourrage d'urne, qui consiste à émettre de multiples témoignages fallacieux en bien ou en mal à l'endroit de l'agent visé [98].

Il existe d'autres attaques visant des algorithmes ou des architectures. L'exemple le plus populaire est celui des « Google bomb » [115]. Cette technique exploite l'algorithme « PageRank » utilisé par le moteur de recherche Google, donnant un score au texte source contenant un hyperlien vers une autre page. Plus nombreux sont les sites utilisant un même texte source, plus élevé sera ce score. À partir d'un certain score, la page vers laquelle pointe le lien apparaît dans les résultats lors d'une recherche du texte source, même si ce texte n'existe pas dans la page obtenue. En pratique, un attaquant peut utiliser une multitude de sites web et les faire pointer vers un même site (par exemple http://www.example.com) en utilisant un même texte source (par exemple « ce site est magnifique »). En cherchant « site magnifique » dans Google, le site http://www.example.com apparaîtra dans les résultats même s'il ne contient ni le mot « site », ni le mot « magnifique ». Ce genre de techniques est appelé « attaques contre le score de réputation par manipulation des critères d'évaluation ». Un attaquant peut vouloir médire sur un fournisseur de service en apportant des témoignages de mauvaise qualité. Ces attaques par médisance peuvent être amplifiées si l'attaquant peut se créer de nombreuses identités, par exemple grâce à une attaque de Sybil réussie ou via une collusion. Enfin, un attaquant peut également essayer de réfuter une transaction où le fournisseur de service s'est bien comporté pour éviter d'avoir à émettre un témoignage positif.

3.2 Attaque générique contre les systèmes distribués

Dans une architecture centralisée, la sécurité du système repose sur la sécurité du serveur central. Si ce dernier est compromis, c'est tout le système qui l'est. C'est de ce fait le point unique de défaillance de ce type de système. Dans les systèmes distribués, la réalité est tout autre, Urdaneta et al. [116] ont présenté trois principales attaques possibles dans les réseaux sous-jacents: l'attaque de sybil, l'attaque d'éclipse et l'attaque sur le routage.

L'attaque de Sybil permet à un attaquant de contrôler plusieurs nœuds du réseau. Dans un réseau, cela lui permet par exemple de router un paquet où bon lui semble.

L'attaque d'éclipse corrompt la table de routage d'un nœud honnête pour s'assurer que les paquets passeront par un nœud contrôlé. Le nœud honnête est alors « éclipsé » puisque la plupart de ses communications peuvent être modifiées par un autre nœud.

Les attaques de routage consistent principalement à ne pas retransmettre ou à modifier les requêtes. Leur impact est augmenté si elles sont combinées avec des attaques de Sybil et d'éclipse.

La plupart des solutions aux attaques d'éclipse et de routage ou de stockage qui sont présentées dans [113, 116-118] font intervenir des chemins multiples, afin de réduire les problèmes concernant le réseau sous-jacent. En effet, l'algorithme de Chord [119] qui permet aussi de contrer ce type d'attaques est déjà robuste de par sa construction, mais sa robustesse peut être améliorée pour tolérer plus d'attaques comme le montre Artigas et al. [120] et Fiat et al. [121]. L'augmentation du nombre de chemins permet l'augmentation de la robustesse.

Un autre problème qui se pose lors des communications dans un réseau distribué est celui de la gestion des identités. En effet, il est parfois nécessaire d'être sûr de l'identité de l'agent avec lequel il communique. Marti et Garcia-Molina [97] proposent à cet effet des techniques de clé publique/privée pour éviter le vol d'identité. Néanmoins, ce système n'est fiable que s'il existe une tierce partie de confiance, un serveur centralisé faisant office d'autorité de certification(CA) et générant des certificats sur les clés publiques.

3.3 Exemple de système de réputation

Les systèmes de réputation peuvent être classés selon leur niveau de complexité en partant des systèmes les plus simples basés sur le vote des participants, vers des systèmes utilisant des algorithmes complexes tels que les systèmes utilisés par Google avec PageRank. Dans la suite, nous présentons le fonctionnement de trois exemples de système de réputation. Il s'agit du système de notation des pages de Google, PageRank, le système de réputation utilisé par McAfee dans les laboratoires McAfee Labs pour la sécurisation des entités électroniques et enfin le système de réputation d'eBay plate-forme de commerce électronique.

3.3.1 Système de réputation PageRank de google

PageRank présenté dans la Figure 3-1 est un système de notation de page web mis en place par Larry Page et Sergey Brin [122] et utilisé par le moteur de recherche Google pour référencer les pages web à travers le monde. Le système PageRank utilise un algorithme basé sur des calculs probabilistes qui permet de noter les pages selon le nombre d'hyperliens auxquels celle-ci est référée et selon le poids des hyperliens qui mènent vers cette page. Le calcul du poids est fait de tel enseigne que plus un hyperlien fait l'objet de citation plus son poids augmente et de ce fait il a une bonne réputation et est donc susceptible d'apparaitre en haut de liste lorsqu'une recherche est réalisée sur des mots qui appartiennent à son contenu ou au contenu des pages qui ont été dirigées vers elle. De plus le poids d'une page est proportionnel aux poids des pages qui l'ont cité. De fait plus les pages de hauts poids citent une page plus cette dernière à un poids élevé. C'est ce qui explique qu'une page citée moins de fois par des pages de très haut poids est mieux noté qu'une page citée plus de fois par des pages de poids faible. Le brevet Google [123] indique que les critères utilisés pour définir le score de réputation d'une page sont les suivants : les liens entrants et sortants, les ancres, le trafic associé à la page, le comportement des internautes (c'est-à-dire le choix de la page dans les résultats), le nom de domaine et l'hébergement. Le système PageRank est un exemple intéressant de réputation où les citations d'autres pages augmentent la fiabilité d'une autre page.

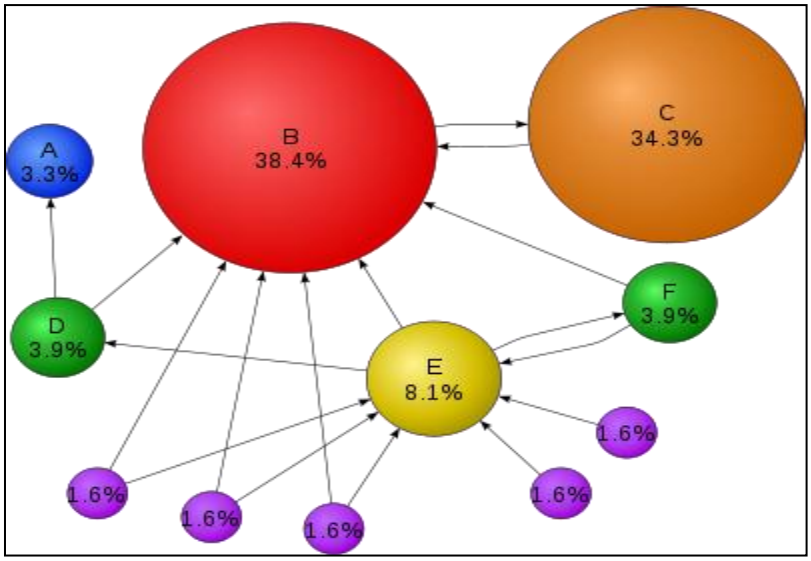

Figure 3.1: Système Page Rank

3.3.2 Système de réputation de McFee Labs

Dans [102], Jamie Barnett présente le système de réputation implémenté dans les laboratoires McAfee Labs pour la sécurisation des données et des entités électroniques. En effet, McAfee calcule la réputation de centaines de millions d'entités électroniques — fichiers, sites et domaines web, messages électroniques, serveurs DNS et connexions réseau — au moyen d'un système de scores de réputation hautement granulaire reposant sur quantité d'informations relatives au comportement et aux caractéristiques de l'entité, ainsi que sur leur propre expérience du comportement d'entités comparables. Entre autres entrées, ils s'appuient sur les données télémétriques obtenues par le biais de milliards de requêtes lancées chaque jour par des dizaines de millions de produits McAfee (clients antimalwares, passerelles de l'environnement web et de la messagerie électronique, pare-feux, etc.) déployés aux quatre coins de la planète et qui servent de sondes pour leur moteur d'analyse dématérialisé. Par exemple, lors du calcul dynamique du score de réputation d'une connexion réseau, ils examinent des milliers d'attributs et de comportements, tels que la durée de vie de l'adresse IP, les ports et protocoles qu'elle utilise, l'activité du réseau par rapport à une ligne de base de comportements attendus, l'historique des attaques et les liens avec d'autres adresses IP connues. Leur système de réputation donne des scores conduisant à quatre niveaux de risques possibles : faible, non-vérifié, moyen, élevé. Ce qui implique que leur système de réputation n'est donc pas binaire. Il constitue trois zones, la zone blanche pour les entités réputées fiables et intègres, la zone noire pour les entités réputées

malveillantes, et une zone grise pour les autres entités, ayant un comportement qui change et qui évolue très rapidement. La fiabilité du système de réputation de McAfee est renforcée grâce à quatre facteurs que sont : le volume, la longévité, la fiabilité des données et la mise en corrélation d'un volume important de données. Un modèle de trafic est défini pour chaque type d'entité, si une activité ne respecte pas ce modèle de trafic celle-ci est donc soupçonnée d'intentions malveillantes.

3.3.3 Système de réputation d'eBay

Avant de participer à une enchère, chaque participant, vendeur ou acheteur doit s'enregistrer en fournissant un certain nombre d'information à eBay [99]. La seule information qu'eBay vérifie est la validité de l'email de l'utilisateur. Lors de l'enregistrement, l'usager choisi un pseudonyme ou un identifiant. C'est cet identifiant qui est montré aux autres membres participants à la transaction. Toutes les informations personnelles révélées à eBay restent confidentielles. Ainsi avec la facilité d'acquérir une adresse email gratuitement sur Yahoo ou Hotmail, chaque usager d'eBay peut rester totalement anonyme vis-à-vis de tous les autres participants. Les vendeurs et les acheteurs peuvent laisser des commentaires les uns sur les autres à la fin de chaque transaction. De plus ils ont la possibilité de laisser une note, +1 (note positive), -1 (note négative), 0 (neutre). Un calcul simple est effectué sur la note qui est donné par les utilisateurs. La valeur totale de la note est considérée en soustrayant les valeurs positives des valeurs négatives. Depuis l'an 2000, les usagers ne peuvent laisser une note que pour les transactions pour lesquelles ils ont été acteurs. Ce si permet d'empêcher à n'importe quel usager de laisser une note. De plus, l'usager peut décider de rendre ses notes invisibles pour tous les usagers. Lorsqu'un usager cherche un item, il voit la liste des items avec le titre et le prix. Dans ce premier affichage, il n'est pas possible de voir le pseudonyme ni le score de réputation. Ce n'est que lorsque l'acheteur clique sur le résumé qu'il peut voir les scores de réputation qui peut être positif, neutre ou négatif. De plus l'utilisateur peut voir le pseudonyme et les commentaires laissé par d'autres usagers à propos des transactions effectuées avec ce vendeur ou acheteur, et aussi le temps écoulé depuis la transaction. Toutes ces informations permettent à l'usager de se faire une opinion sur son prochain partenaire. En réalité dans ce système de réputation, c'est l'usager qui prend la décision au vu de toutes les informations qu'il a à sa disposition.

3.4 Différents types de réputation

Dans la littérature, Le concept de réputation a été abordé selon différentes approches et dans des contextes différents les uns par rapport aux autres. De ce fait différents types de réputation ont été présentés, Notamment en ce qui concerne les applications de e-commerce et P2P et aussi dans les réseaux Mobiles Ad-hoc et les réseaux de capteurs [107, 123-125]. Dans cette section, nous présentons en premier lieu, le but et les propriétés des systèmes de réputation, ensuite, nous présentons les différents types de réputation.

3.4.1 Système de réputation : les buts et les propriétés

Dans [106] et [99] , les auteurs présentent le but des systèmes de réputation dans les réseaux auto-organisés : (i) permettre aux nœuds de faire la distinction entre les nœuds honnêtes et les nœuds malicieux dans le réseau, (ii) encourager les nœuds du réseau à coopérer les uns avec les autres, (iii) décourager les nœuds malicieux à participer aux activités du réseau, (iv) permettre aux systèmes de réputation de gérer tous les types de mauvais comportement des nœuds du réseau et (v) de minimiser les dommages causés par une attaque perpétrée par un nœud.

Afin d'opérer de façon efficiente, les systèmes de réputation dans les réseaux sans-fil doivent avoir les propriétés suivantes [126] : le système doit posséder une entité qui permet de prévoir les interactions futures, le système doit être à même de capturer et de distribuer le feedback à propos des interactions courantes entre les différents acteurs du réseau et ces informations devront être disponibles dans le futur. Et enfin, le système devrait s'inspirer des feedbacks sur les évènements précédents pour pouvoir prendre sa décision.

3.4.2 Les types de réputation

La classification des systèmes de réputation peut être effectuée selon différentes approches. Les systèmes peuvent être classés selon plusieurs critères : Initialisation du score de réputation, le type d'observation qui est utilisé, la manière donc les observations sont exploitées, la façon donc les informations sont distribuées à travers le réseau [99]. La majorité des systèmes de réputation sont initialisés de la façon suivante :

a- Tous les nœuds du réseau sont initialement considérés comme étant fiables. Chaque nœud a confiance à ces voisins. Le score de réputation de chaque nœud décroit s'il agit de façon répréhensible.
b- Chaque nœud du réseau est considéré comme non fiable au démarrage du réseau. Ainsi les nœuds n'ont pas confiance les uns aux autres. Le score de réputation augmente au fur et à mesure que les nœuds démontrent leur bon comportement.
c- Chaque nœud du réseau est considéré ni fiable ni non fiable au démarrage du réseau. Chaque nœud démarre donc avec un score de réputation neutre. Le score de réputation changera selon le bon ou le mauvais comportement du nœud.

Sur la base des observations qu'ils utilisent, les systèmes de réputation peuvent être classés en deux groupes : (i) les systèmes utilisant les informations locales encore appelé information de première main, (ii) les systèmes utilisant à la fois les informations de première main et de seconde main pour construire une opinion. Pour les systèmes utilisant seulement les informations de première main, la décision et le score de réputation sont définis en exploitant les informations provenant des observations réalisées localement, alors que les systèmes qui utilisent les deux types d'informations exploitent non-seulement les informations provenant des observations locales mais aussi celles provenant des observations provenant des voisins. La majorité des systèmes actuels de réputation prennent en compte les observations de première et de seconde main. Dans ce cas, les systèmes ont plus d'information pour pouvoir construire le score de réputation et de prendre les bonnes décisions. Les systèmes pour lesquelles seules les observations locales sont exploitées ont l'avantage d'échapper aux attaques de diffusion de faux témoignages. Deux exemples de ce type de systèmes sont présentés dans [107] et [104]. Certains types de systèmes de réputation n'utilisent que les informations de seconde main pour construire les métriques de réputation [127]. Dans ce type de systèmes de réputation, les nœuds n'ont pas au préalable des observations collectées localement. Une façon de gérer ces systèmes de réputation est de rendre disponible sur les réseaux les observations de tous les autres nœuds.

Une autre façon de catégoriser les systèmes de réputation est de les distinguer selon la façon dont ils accèdent aux observations sur le réseau. (i) les systèmes symétriques, (ii) les systèmes asymétriques. Dans les systèmes de réputation symétriques, tous les nœuds du réseau ont accès au même niveau d'information, que ce soient les informations de première main ou de seconde main. Dans les systèmes de réputation asymétriques par contre, tous les nœuds n'ont pas accès

au même niveau et à la même quantité d'information. Par exemple dans [127], les nœuds du « Node Sink » (SN) n'ont pas accès à des observations de première main. Cette contrainte peut être un inconvénient pour les nœuds qui ne disposent pas d'assez d'informations pour prendre la bonne décision.

La distribution de la réputation à travers le réseau peut permettre de catégoriser les systèmes de réputation : (i) Centralisée, (ii) Distribuée. Dans les systèmes centralisés, une entité centrale maintient les scores de réputation de tous les nœuds du réseau. Cette entité centrale peut être source de vulnérabilité en termes de sécurité. Parmi les exemples de ce type de système de réputation, nous pouvons citer les sites d'enchère eBay ou encore Yahoo. Dans les systèmes distribués de réputation, chaque nœud peut maintenir les scores de réputation des nœuds de son voisinage ou encore maintenir les scores de réputation de tous les nœuds du réseau. Dans les réseaux de capteurs, chaque nœud maintient seulement les informations de réputation de son voisinage. Cette disposition réduit considérablement les problèmes de manque de mémoire de stockage.

3.5 Réputation dans les réseaux ad-hoc mobiles

Les systèmes de réputation peuvent être appliqués dans les réseaux Ad-hoc Mobiles afin de doter les nœuds de moyens pour se protéger contre d'autres nœuds qui s'avèreraient malicieux. Dans cette partie, nous présentons comment se fait l'intégration de systèmes de réputation dans les réseaux Ad-hoc Mobiles.

3.5.1 Généralités

Les réseaux ad-hoc mobiles sont composés de participants ayant minimalement les mêmes caractéristiques en termes de ressources. Ce sont des nœuds qui communiquent de manière décentralisée à travers un réseau sans-fil. Pour ces réseaux, l'on peut considérer aussi bien les communications à plusieurs sauts que les communications directes entre nœuds voisins [96]. Ces réseaux ont pour particularité de dépendre fortement les uns des autres. De ce fait, il est important de s'assurer de l'effectivité des tâches effectuées par chaque participant du réseau en évitant des comportements égoïstes par des nœuds. Ou encore des attaques potentielles du fonctionnement global ou d'une tâche particulière. Pour mener à bien ces tâches, chaque entité réseau observe le comportement de ses voisins en utilisant la technique de réputation. Le bon fonctionnement des

réseaux Ad-hoc mobiles repose sur la confiance entre les différents participants du réseau. Hors cette relation de confiance n'est pas toujours acquise dans un réseau ad-hoc. Dans les conditions normales, une simple authentification devrait être suffisante pour assurer le bon fonctionnement du réseau. Malheureusement, il se peut que certains nœuds aient des intentions malicieuses. Un système où règne une confiance aveugle entre les nœuds n'existe que dans les réseaux propriétaires. Par exemple les réseaux militaires, ou certains réseaux d'entreprises [128]. Le bon fonctionnement des réseaux auto-organisés dépend grandement du bon comportement de tous les acteurs de ce réseau. Car chaque acteur doit effectuer des tâches précises pour que tous les paquets circulent dans le réseau de façon fluide.

Dans le cas de l'existence de nœuds malicieux au sein du réseau, il faut trouver une méthode efficace pour sécuriser les données. Il est légitime de penser à l'utilisation des méthodes de sécurisation classiques des réseaux. Malheureusement, ceux-ci ne sont pas efficacement applicables aux réseaux mobiles ad-hoc, notamment les VANETs qui sont des réseaux hautement mobiles. Les participants des réseaux auto-organisés peuvent mal se comporter et ainsi nuire au bon fonctionnement du réseau pour deux types de raisons : (a) les raisons intentionnelles, (b) les raisons non-intentionnelles.

Parmi les raisons intentionnelles, nous pouvons citer l'économie d'énergie. Un nœud voulant conserver son énergie agira de façon égoïste et ne collaborera pas au bon fonctionnement du réseau. Ce type de comportement survient dans les cas où l'énergie constitue une denrée rare. Par exemple les réseaux de capteurs. D'autres nœuds peuvent tout simplement vouloir nuire au bon fonctionnement du réseau en refusant de collaborer (par exemple pour le relais des informations) ou encore en injectant des informations dangereuses dans le réseau (actions malicieuses).

Les raisons non-intentionnelles surviennent lorsque le nœud se retrouve à cour d'énergie ou subit une panne de son système ou encore une panne du lien de communication (par exemple batterie déchargée d'un senseur ou encore coupure de liaison réseau entre deux nœuds).

3.5.2 Les objectifs d'un système de réputation

Le système de réputation a deux objectifs :

- permettre aux nœuds de trouver les meilleurs partenaires de communication

- donner à ceux-ci une raison de coopérer (par exemple pour le routage des informations).

Ces deux objectifs englobent les challenges qui guettent tous les réseaux auto-organisés. Notamment le partage des informations et des ressources du réseau pour un objectif commun de bonne marche du réseau. Malheureusement, ces objectifs ne sont pas facilement atteignables, car les instances de coopération dans le réseau n'ont pas tous intérêt à aider au fonctionnement du réseau. Certains nœuds préfèrent profiter des ressources du réseau sans apporter de contributions; d'autres nœuds par contre souhaitent tout simplement nuire au bon fonctionnement du réseau. Il est donc nécessaire de se rassurer de l'envie de coopération qui anime les acteurs du réseau et surtout se rassurer des opportunités que leur apporte cette coopération.

3.6 Les métriques d'honnêteté dans un système de réputation

Les métriques d'honnêteté d'un système de réputation varient d'un environnement à un autre dépendamment des objectifs fixés. De plus, la construction de celles-ci impose une étude sérieuse et approfondie des outils utilisés pour arriver au résultat qui déterminera la prise de décision. Dans cette partie, nous présentons certains travaux dans lesquels les métriques de réputation ont été construites dans le but de la sécurisation des MANETs.

Qing Ding et al. [129] proposent un système de réputation ayant pour objectif de filtrer les messages envoyés par les nœuds malicieux. De ce fait, ils catégorisent les nœuds du réseau en trois groupes :

1. les reporteurs d'évènement (ER : Event Reporter), ce sont des nœuds qui sont capables de détecter la présence d'un incident grâce à leurs capteurs et ainsi peuvent envoyer un message d'alarme à leur voisinage.
2. les observateurs d'évènement (EO : Event Observer), Ce sont des nœuds qui sont proches du ER et qui sont capables d'observer le comportement de ce dernier.
3. et enfin les participants à l'évènement (EP : Event Participant), Ce sont des nœuds qui sont positionnés loin des ER, ils peuvent seulement transférer les messages envoyés par ces derniers, mais ne peuvent observer leur comportement.

Les auteurs collectent les informations sur l'environnement des nœuds grâce à des équipements tels que les interfaces sans-fil et les capteurs embarqués. Chaque nœud dispose d'une table d'enregistrement des évènements ayant les informations telles que : l'ID de l'évènement, le type de l'évènement, le timestamp de l'occurrence, la localisation de l'évènement, le rayon de transmission et la valeur de réputation. Selon la gravité de l'évènement détecté par le ER, celui-ci décide de le transmettre au voisinage selon la valeur de réputation associé à cet évènement. L'information sera donc collectée par les observateurs d'évènements qui ne sont autres que les nœuds voisins à un saut. Les EO enregistrent le message d'évènement dans une table d'évènement et observent ensuite le comportement de l'ER qui a envoyé le message. Si ce dernier respecte le comportement attendu alors la valeur de réputation concernant ce message est notée positivement et le message est considéré comme fiable. Dans le cas contraire, le message est considéré comme indésirable. De plus, l'EO observe aussi les messages provenant d'autres EOs et d'autres ERs. Si l'information est cohérente le message est considéré fiable, sinon, il est considéré comme indésirable.

Pietro et Refik [128] ont présenté le protocole CORE (Collaborative Reputation Mechanism to enforce node cooperation in Mobile Ad Hoc Networks) dans lequel ils définissent trois types de réputation: la réputation subjective qui traduit les informations collectées de façon locale par un nœud, la réputation indirecte qui prend en compte les observations réalisées par d'autres nœuds du voisinage et la réputation fonctionnelle qui s'intéresse à une fonction précise du système.

La réputation subjective

Le terme réputation subjective est utilisé pour parler de la réputation calculée localement par le nœud hôte. On parle alors d'observation subjective. Une réputation subjective à un temps t par un nœud s_i est calculée en utilisant la moyenne pondérée des facteurs d'observation en donnant plus d'importance aux observations passées. Dans le modèle CORE, plus de pertinence est donnée aux observations passées à cause d'une éventuelle inconsistance des récentes observations. Dans le cadre des réseaux VANETs, cette hypothèse n'est plus valable car les nœuds se déplacent à une vitesse très élevée et l'analyse se fait sur des données récentes. La formule générale du calcul du score subjectif de réputation proposé dans le modèle CORE est la suivante:

$$r_{s_i}^{t}(s_j|f) = \sum \rho(t, t_k) \cdot \sigma_k$$

Ou $r_{s_i}^{t}(s_j|f)$ représente la valeur de réputation subjective calculée à l'instant *t* par le nœud hôte s_i à propos du nœud visiteur s_j en respectant la fonction *f*.

$\rho(t, t_k)$ représente la fonction de temps qui permet de donner une plus grande pertinence à la valeur des observations.

ρ_k représente le facteur de notation attribué à la k_{ieme} observation. L'on utilise un intervalle qui part de -1 pour une impression négative (signifiant que l'observation ne correspond pas au résultat espéré), à +1 pour une impression positive (qui signifie que l'observation correspond au résultat attendu). Lorsque la quantité et la qualité des observations collectées depuis le temps *t* ne sont pas suffisantes, la valeur de réputation subjective finale prend la valeur 0 qui exprime une impression de neutralité.

Finalement, en considérant que $\rho_k \in$ [-1,1] et que $\rho(t, t_k)$ est une valeur normalisée, alors $r_{s_i}^{t}(s_j|f) \in$ [-1,1].

L'ensemble s_j est considéré comme l'ensemble des voisins du nœud *i*, le voisinage de *i* est constitué de tous les nœuds qui sont dans le même rayon de transmission que *i*.

La réputation indirecte

Dans la partie précédente, il était question d'une réputation subjective, prenant en compte seulement les observations collectées par le nœud lui-même. Mais dans la réalité, les choses ne sont pas aussi simples. Dans certaines situations, l'on considère les observations collectées par les nœuds voisins. La réputation indirecte est donc constituée des observations faites par le nœud hôte et celles faites par d'autres nœuds (nœuds voisins préalablement considérés comme honnêtes). On la note: $ir_{s_i}^{t}(s_j|f)$: Réputation indirecte sur le nœud visiteur *j* par le nœud hôte *i* à l'instant *t* en suivant la fonction *f*. Quelques précautions doivent être prises lors de la collection des informations pour une réputation indirecte. Par exemple, l'on pourrait considérer seulement les notations positives pour éviter que des dénis de service perpétrés par des nœuds malicieux ne soient effectifs et contribuent à une note négative des nœuds légitimes et honnêtes. Une prise en compte du fait, que des nœuds malicieux se concertent afin de noter positivement d'autres nœuds négatifs, est à faire. Sinon, ceci contribuerait à avoir des cas de faux négatifs.

La réputation fonctionnelle

Le terme de réputation fonctionnelle est utilisé pour représenter le cas où les réputations subjective et indirecte sont calculées en respectant une fonction différente *f*. Ce type de réputation donne la possibilité de calculer une valeur globale de réputation d'un sujet en prenant en compte des critères d'observation et d'évaluations différentes. Par exemple, le nœud hôte s_i peut évaluer la réputation subjective : $r_{s_i}^t\left(s_j|f(packet\ forwarding)\right)$ d'un sujet s_j en respectant la fonction de transfert de paquets et la réputation subjective $r_{s_i}^t\left(s_j|f(routing)\right)$ en respectant la fonction de routage et ensuite les combiner en utilisant différents poids pour obtenir une réputation globale du nœud s_j .

Les informations de réputation sont combinées en utilisant la formule suivante:

$$r_{s_i}^t(s_j) = \sum w_k \cdot \{r_{s_i}^t(s_j|f_k) + \mathrm{i}r_{s_i}^t(s_j|f_k)\}$$

où w_k représente le poids associé à la valeur de la fonction de réputation.

$r_{s_i}^t(s_j)$ représente la valeur globale de réputation évaluée par chaque nœud. C'est l'agrégation de toutes les valeurs de réputation. Le choix de w_k est primordial pour la pertinence de la valeur de réputation globale finale. Il est donc important de faire un choix raisonnable de cette variable.

Le choix du modèle pour la construction des métriques de réputation dans les réseaux ad-hoc mobile dépend des objectifs fixés par le concepteur du système. Dans cette section, nous avons présenté deux modèles de construction des métriques de réputation. Globalement, tous les systèmes de réputation visent la sécurisation et le bon fonctionnement des réseaux.

3.7 Conclusion

Dans ce chapitre, nous avons présenté le concept de réputation et des systèmes de réputation, les catégories de systèmes de réputation ont aussi été abordées, les systèmes de réputation peuvent être catégorisés de plusieurs façons selon différentes caractéristiques. L'architecture des systèmes de réputation a aussi été abordée, un système de réputation doit disposer d'un processus d'observation, un processus de stockage des observations, un processus de traitement et un processus de prise de décision. Nous avons présenté trois exemples de systèmes de réputation.

L'algorithme « PageRank » qui est utilisé par le moteur de recherche Google, les solutions anti-virus de McAfee et la plate-forme de commerce électronique eBay. Ces exemples montrent que les systèmes de réputation sont des outils efficaces à la prise de décision de situations aussi différentes que de savoir quelle page web afficher en haut de page pour une recherche par mot clé. La sécurisation des entités électroniques par l'observation d'un modèle de communication et de comportement des différents acteurs. Et enfin la capacité d'assurer aux utilisateurs d'une plate-forme de commerce électronique, la fiabilité des différents participants aux transactions. Quelques modèles sur la construction des métriques de réputation pour les réseaux mobiles ad-hoc ont aussi été abordés. Le modèle CORE qui est un modèle conçu pour la sécurisation des réseaux ad hoc mobiles donne des formules pour la construction des métriques de réputation en divisant les scores de réputation en trois groupes, la réputation subjective, la réputation indirecte et la réputation fonctionnelle. Nous nous inspirerons de ces travaux pour mettre en place le système de réputation que nous proposons pour la sécurisation des VANETs dans le chapitre suivant.

CHAPITRE 4

SYSTÈME DE SÉCURISATION DES VANETS PAR RÉPUTATION (SSVR)

Les VANETS (Vehicular Ad-Hoc Networks) sont considérés comme un ensemble de véhicules qui communiquent les uns avec les autres dans un environnement de transport publique. En fait les véhicules sont dotés d'un ensemble d'équipements qui leurs confèrent la capacité de réaliser un certain nombre d'actions telles que : collecter des informations sur leur environnement proche grâce aux senseurs et aux radars, savoir à chaque instant la position géographique à laquelle ils se trouvent grâce au GPS (Global Positioning System) et la distance des voisins les plus proches, être capable de communiquer les uns avec les autres grâce aux équipements de communications intégrés comme les antennes de communication, une plate-forme de transmission, etc. Les véhicules sont de ce fait intelligents. Ils sont d'ailleurs dotés d'un ordinateur de bord qui permet de traiter toutes les informations collectées par les différents équipements. Cette intelligence accrue dans les véhicules permet aux chercheurs de penser à un nouveau type de réseau informatique, un réseau qui permettrait à un ensemble de véhicules de se partager les informations sur la route de façon à rendre les routes plus sécuritaires, à rendre l'expérience de conduite ou de voyage en automobile plus conviviale et globalement de rendre le système des transports plus fiable. Ces réseaux véhiculaires trouvent d'ailleurs leur origine dans un type de réseau appelé MANET (Mobile Ad-hoc Networks) qui existait déjà. Les VANETs apportent de nombreux avantages pour les usagers de la route, car grâce à eux, plusieurs applications pourraient voir le jour. Malheureusement il s'agit toujours de réseaux informatiques, qui sont soumis à des menaces de sécurité des données transmises et même du réseau sous-jacent. Dans ce cas précis, toutes les brèches de sécurité encourues par les MANETs se trouvent reportées aux VANETs. En plus, il existe d'autres brèches de sécurité inhérentes au cas particulier des VANETs, par exemple l'attaque d'illusion, l'attaque de l'homme du milieu, etc. C'est la raison pour laquelle les exigences en termes de sécurité sont plus grandes dans ces derniers. Des précautions ont été prises pour la sécurisation des messages transmis dans les VANETs notamment sur les protocoles utilisés pour la transmission des informations[28].

Depuis quelques années, une activité de recherche intense est menée par les chercheurs à travers le monde, ainsi plusieurs architectures, protocoles, algorithmes ont été proposés pour la sécurisation des VANETs. Certains chercheurs se sont concentrés sur la sécurisation des

messages transmis notamment par des méthodes de cryptage par certificat et clé public/privé. D'autres par contre ont jeté leur dévolu sur la sécurisation des protocoles : les protocoles de dissémination des messages, les protocoles de routage des messages, etc. Une autre catégorie de chercheur s'est concentrée sur l'authentification et le filtrage des véhicules dans le réseau. Parmi ces derniers, il y en a certains qui ont choisi la sécurisation par la méthode de réputation. La réputation que nous avons présentée au chapitre précédent, est un concept qui est basé sur l'expérience et la confiance qui en découle. En effet avant d'accepter une communication avec un nœud qui demande à communiquer, le nœud hôte doit se rassurer de la réputation du nœud visiteur grâce à une série de vérification réalisée par lui-même et par ses voisins et ceci grâce à l'expérience des communications précédentes.

Dans notre travail, nous avons élaboré un système de réputation, SSVR (Système de Sécurisation des VANETS par Réputation), que nous intégrons dans chaque nœud participant au réseau lui permettant de faire les analyses nécessaires, grâce à un algorithme, et ainsi de prendre la bonne décision quant au choix d'accepter ou non, de communiquer avec le nœud visiteur. En effet, nous collectons d'une part les variables annoncées par le nœud telles que : l'identifiant du nœud, la vitesse de déplacement du nœud, la position géographique du nœud, la direction du nœud, l'accélération. D'autres parts, nous exploitons certaines variables qui sont calculées par le nœud récepteur telles que : la fréquence de transmission et le rayon de transmission. Ces variables sont ensuite analysées de façon à déterminer si le nœud visiteur est honnête ou non. Chaque nœud ayant une mauvaise réputation est éjecté du réseau et celui ayant une bonne réputation devient un partenaire de communication. Ceci permet donc de lutter contre certaines attaques telles que les attaques sur la position, les attaques de sybil, les attaques d'usurpation d'identité, les attaques de déni de service ou encore les attaques d'illusions.

Ce système, non seulement sécurise les réseaux VANETs, mais il permet aussi d'analyser le comportement des usagers sur la route. Il peut donc aussi être utilisé comme un outil forçant les usagers de la route à mieux se comporter sous peine de ne pouvoir profiter des avantages que leur confère le réseau.

Notre principale contribution dans ce travail est de montrer qu'en exploitant tous les nouveaux équipements tels que les radars, les GPS, les Event Data Recorder (EDR), nous

pouvons détecter les nœuds qui mentent sur certaines données qu'elles fournissent à leur voisinage et ainsi les éjecter du réseau.

Ce chapitre est divisé comme suit : dans la section 4.1, nous présentons les requis du système, en section 4.2, il est question du modèle du système, dans la section 4.3, nous présentons l'architecture proposée, dans la section 4.4, se fait la présentation des modules du système, la section 4.5 expose le modèle binaire, la section 4.6 expose le modèle flexible, dans la section 4.7, on définit mathématiquement le système proposé, en section 4.8 l'algorithme binaire exploité pour le fonctionnement du système est présenté, la section 4.9 présente l'algorithme flexible exploité pour le fonctionnement du système.

4.1 Les requis du système

Les systèmes de réputation sont utilisés dans les domaines aussi variés que les sciences sociales, l'économie, l'informatique et particulièrement dans l'intelligence artificielle ou encore les réseaux mobiles. En ce qui concerne les réseaux mobiles, ils sont utilisés pour la sécurisation des réseaux auto-organisés. Le but d'un système de réputation est surtout d'aider à la prise de décision en dotant les usagers d'une capacité à déterminer la confiance d'un interlocuteur. Ces systèmes pour être fiables doivent disposer des caractéristiques suivantes : intégrer un processus d'observation, un processus de stockage de ces observations, un processus de traitement et un processus de prise de décision.

4.2 Les modèles du système

Cette section présente les différentes entités qui constituent notre système de réputation. Dans un premier temps, nous présentons le modèle du véhicule, qui indique les équipements dont ce dernier est doté pour permettre l'implémentation du système de réputation. Ensuite, nous présentons le modèle du réseau qui indique la topologie réseau dans laquelle les véhicules évoluent, et enfin nous présentons le modèle de l'attaquant. Dans cette partie nous décrivons les caractéristiques d'un attaquant.

4.2.1 Le modèle du véhicule

Jean Pierre Hubaux et al. [130] ont proposé un modèle de véhicule constitué d'un certain nombre d'équipements et d'un ensemble de processeurs connectés à un ordinateur central, avec

des connecteurs Ethernet, wifi, Bluetooth, USB et une interface de communication IEEE 802.11, qui permettent à un véhicule d'avoir une certaine intelligence. C'est ce modèle de véhicule que nous prenons en considération dans la réalisation de notre travail. En effet, ce véhicule est constitué des équipements suivants :

- Un enregistreur des données des évènements (EDR : Event Data Recorder). C'est un équipement inspiré de la boite noire dans les avions. Il enregistre toutes les informations durant tout le voyage et peut aussi aider à la reconstruction des évènements précédents un accident.
- Un récepteur GPS (Global Position System) permet de connaître la position du véhicule et la topologie de la route à tout instant.
- Des radars avants et arrières permettent de détecter les obstacles jusqu'à une distance de 200 mètres.
- Une interface de communication Wifi prend en compte les signaux DSRC (Dedicated Short Range Communication) et sont dédiés aux communications rapides spécialisés pour les VANETs.
- Un identificateur électronique unique du même type que la plaque d'immatriculation.

Globalement le véhicule est doté de capacité sensorielle, de mémoire, de traitement de l'information, et de détection de la position géographique, de communication et de comportement adaptatif.

Dans cette recherche, nous allons nous baser sur les travaux de Maxim Raya et al. [131], pour considérer que la majorité des véhicules sur les routes sont honnêtes et se comportent de façon responsable. Les différentes informations exploitées sont considérées comme disponibles grâce aux paquets envoyés par les nœuds qui tentent d'entrer en communication. Et les paramètres de vérifications utilisées par les véhicules qui effectuent l'analyse sont considérées comme disponibles via les différents équipements dont disposent ces véhicules. Il s'agit entre autre des radars, des GPS, des capteurs et aussi des informations déjà collectées par d'autres véhicules du réseau. Le véhicule (émetteur) qui souhaite entrer en communication, sera considéré comme le véhicule visiteur et le véhicule (récepteur) qui est sollicité pour la communication sera appelé véhicule hôte. Dans la suite, puisque nous considérons un environnement réseau, nous utiliserons les termes véhicule et nœud pour nommer les véhicules en communication.

4.2.2 Le modèle du réseau

Nous considérons le scénario de communication d'une autoroute, et nous faisons fi des cas du centre-ville, des zones rurales, des zones résidentielles et tout autre environnement de transport public. Malgré la présence de deux types de cellules dans la littérature pour la modélisation des VANETs, nous considérons seulement le cas des cellules basées sur la position géographique [132]. Ainsi l'ensemble des voisins sera l'ensemble des véhicules présents à l'intérieur du diamètre de la cellule et avec lesquels la communication est établie. Nous considérons que le rayon de transmission de chaque nœud est égal au diamètre de la cellule. Le type de cellule considéré est celui de la figure 4.2 [133]. Tout nœud qui tente d'entrer en communication avec les nœuds du réseau devra transmettre un message du même type que celui de la figure 4.1 proposé par Jyoti Grover et al. [134]. Les variables publiées dans l'entête du message de la figure 4.1 dépend du type d'application. Trois acteurs sont concernés, le nœud hôte, le nœud visiteur et les nœuds voisins au nœud hôte et au nœud visiteur. Les nœuds voisins sont ceux qui appartiennent à la même cellule et qui ont déjà communiqué soit avec le nœud hôte ou le nœud visiteur.

ID	Position	Speed	Time	Direction	Accélération	…	message

Figure 4.1: Structure d'un paquet de type VANET

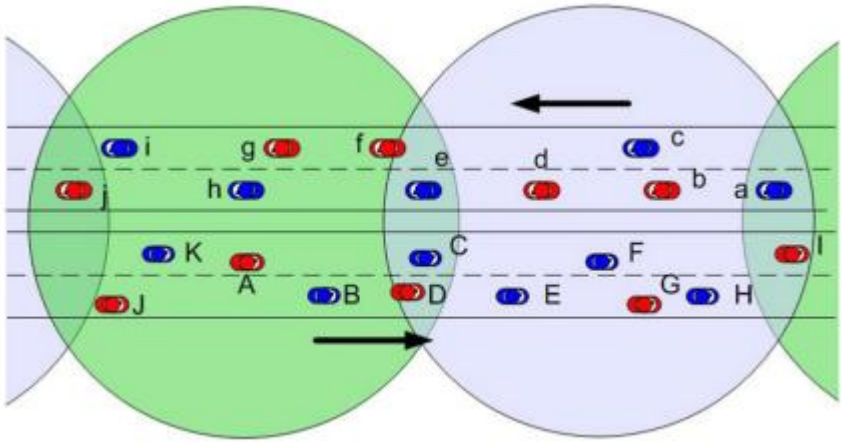

Figure 4.2: Structure d'une cellule VANET

4.2.3 Le modèle de l'attaquant

Dans le cadre de notre travail, nous considérerons comme malicieux tout nœud ayant communiqué des informations qui ne concordent pas avec celles attendues. Chaque nœud voulant faire partie du réseau pour communiquer avec d'autres nœuds devra être soumis au système de réputation intégré dans chaque nœud. Et les informations communiquées seront comparées à un ensemble de paramètres attendus. Dans le cas où l'ensemble des notes obtenues après évaluation des différentes variables correspond à un intervalle de tolérance, alors le nœud est considéré comme honnête, dans le cas contraire, il sera considéré comme malicieux. Tout nœud réputé malicieux, sera intégré dans une liste d'exclusion appelée « liste noire » et ainsi éjecté du réseau.

4.3 Architecture

Dans cette section, nous présentons l'architecture de notre système de réputation. Il est constitué de plusieurs parties qui contribuent au calcul du score global de réputation et donc à la prise de décision qui permettra au nœud hôte d'accepter ou de refuser de communiquer avec un nœud visiteur.

4.3.1 Présentation du parcours d'un paquet

Avant de présenter notre architecture, nous présentons le contexte dans lequel nous considérons que SSVR fonctionnera. En effet, le système de réputation agit à partir de l'interface réseau, entrée/sortie des paquets. Nous considérons qu'un message reçu par le nœud doit passer au travers du système qui est constitué d'un algorithme divisé en plusieurs modules de vérification avant d'être exploité par le VANET. Ainsi, nous présentons le parcours d'un paquet, à partir de son arrivée sur l'interface réseau jusqu'à son exploitation.

La figure 4.3 est une représentation de ce parcours. En effet, le paquet arrive à l'interface d'entrée du nœud. Ensuite, ce dernier est directement soumis au système de réputation qui vérifie que les variables publiées via ce paquet par le nœud visiteur sont conformes aux paramètres attendus par le nœud hôte. Une fois cette vérification terminée, une décision est prise quant à l'acceptation ou le refus du paquet. Si le score des différentes variables est bon alors le paquet peut traverser le système de réputation avec succès et le nœud est donc considéré comme

honnête. Ensuite, l'intégrité des messages est vérifiée par un second module qui en a la charge [73]. Si cette étape est traversée aussi avec succès, alors le paquet peut être exploité sans crainte et une communication entre les deux nœuds peut commencer.

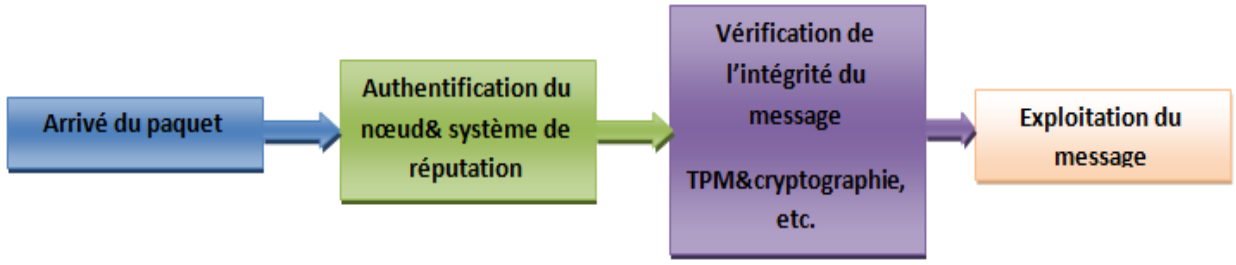

Figure 4.3: Parcours d'un paquet de son arrivé à son exploitation

Selon les cas, l'initiation de la communication se fait en plusieurs phases :

- la phase de découverte du réseau qui est classique pour tous les réseaux ad-hoc. Durant cette phase, le nœud envoie des trames beacon pour découvrir le réseau.
- dans la phase d'acceptation, les trames beacon sont soumises au système de réputation de chaque nœud qui l'a reçu avant que ce dernier l'accepte en tant que voisin.
- la phase de communication effective : si le nœud est accepté, alors il peut partager des informations avec les autres nœuds du réseau.

Une fois le processus d'acceptation réalisé, les échanges peuvent réellement commencer. Par contre un historique de chaque nœud est conservé pour continuer à observer son comportement afin de pouvoir décider lors d'éventuelles communications futures.

4.3.2 Fonctionnement interne de l'architecture proposée

L'architecture proposée pour le système de réputation décrit les différents modules qui le constituent. Il s'agit des variables reçues du nœud visiteur, des listes utilisées pour stocker les identifiants et les différents scores de réputation, les différentes fonctions d'analyses des variables, du module d'agrégation des notes obtenues pour chaque variable par chaque fonction d'analyse, du module d'agrégation des scores de réputation et du module de prise de décision.

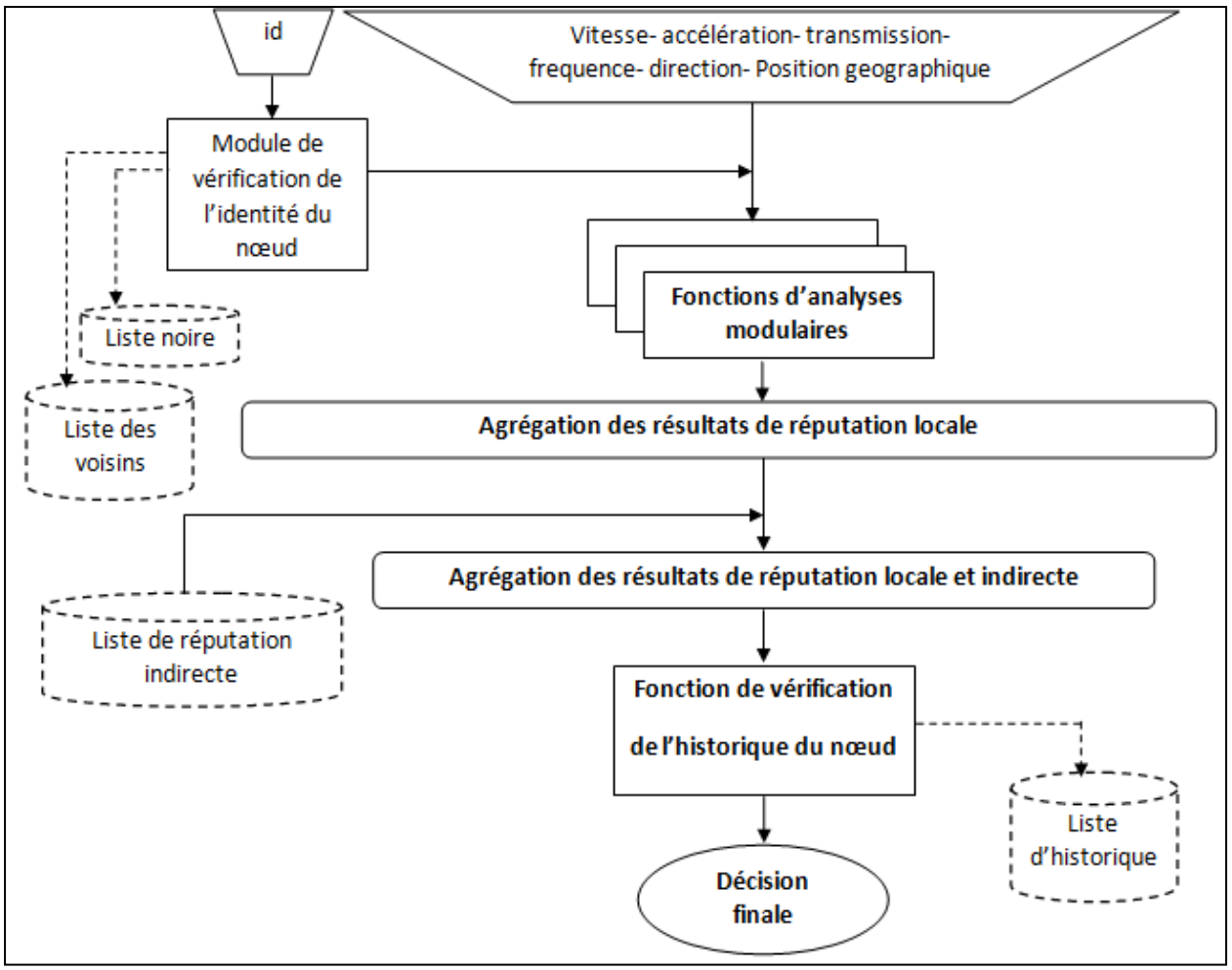

Figure 4.4: Architecture du système de réputation

Selon la figure 4.4, l'architecture du système SSVR, que nous proposons se divise en plusieurs parties **:** les variables fournies par le nœud visiteur, les variables calculées par le nœud hôte, les listes, les fonctions d'analyses pour chaque variable, le module d'agrégation des notes obtenues pour chaque variable afin d'obtenir le score de réputation locale, le module d'agrégation des scores de réputation locale, le modules d'agrégation des scores de réputation locale et indirecte, le module de vérification de l'historique du nœud et le module de prise de décision**.**

4.3.2.1 Les variables

Ce sont les différentes informations qui seront analysées par les fonctions d'analyses pour tester la validité du nœud. Il s'agit de :

- identifiant du véhicule;

- largeur du véhicule en mètre;
- longueur du véhicule en mètre;
- direction du véhicule (1, -1) (1 direction vers le centre de la cellule, et -1 direction en s'éloignant du centre de la cellule);
- position – (x, y) : où x est la position de l'arrière du véhicule et y la position du centre du véhicule;
- vitesse en m/s;
- accélération en m^2/s;
- rayon de transmission est égal au diamètre de la cellule (en mètre).
- fréquence de transmission des paquets dans le VANET(Hz).

4.3.2.2 Les listes

Pour maintenir une trace des nœuds visiteurs avec lesquelles le nœud hôte a été en relation, nous dénombrons plusieurs listes, chacune ayant un rôle spécifique. Il s'agit de :

Liste des voisins : nous conservons les identifiants de tous les nœuds qui sont actuellement en communication avec le nœud hôte. Ces nœuds représentent l'ensemble des voisins.

Liste noire : cette liste stocke les identifiants de tous les nœuds qui ont été considérés comme malicieux par le score de réputation.

Liste d'historique : Cette liste conserve l'historique de tous les nœuds avec lesquelles le nœud hôte a été en communication. C'est-à-dire les informations relatives aux nombres de tentatives de communication ou de communications effectives et le temps du début de la connexion. Ce temps de début de la communication permet de calculer l'âge des informations enregistrées. Nous représentons cet âge par T, qui nous permettra de définir si une information est encore valide ou si elle est obsolète. L'âge se calcule en soustrayant le temps actuel au temps de début de la communication.

Liste de réputation indirecte : elle permet de stocker les scores de réputation que les nœuds voisins ont calculés à propos du nœud visiteur. Les informations contenues dans cette liste sont aussi considérées selon leur âge. Nous représentons aussi cet âge par T. Au-delà de T, les scores contenus dans cette liste ne sont plus valides, ils sont considérés comme obsolètes.

4.3.2.3 Le module de vérification de l'identité du nœud

Ce module a pour rôle de déterminer le statut du nœud visiteur. Le statut du nœud visiteur dépend de ses relations précédentes avec le nœud hôte. Les statuts possibles que peut avoir le nœud visiteur sont les suivants : voisin, malicieux, indéterminé; selon la liste dans laquelle on le retrouve.

Si le nœud fait partie de la liste des voisins, il a le statut de voisin; Dans ce cas, la liste d'historique est vérifiée pour se rassurer que son score n'est pas obsolète. Si le score de réputation n'est pas obsolète, la communication est acceptée. Par contre si le score est obsolète, le nœud est de nouveau soumis au système de réputation pour déterminer son nouveau score de réputation.

Si le nœud a essayé de communiquer et a été détecté malicieux, il fait partie de la liste noire, il a le statut malicieux; il est donc éjecté du réseau.

Si le nœud n'a jamais communiqué, c'est un nouveau nœud dans le réseau, il ne fait partie d'aucune liste, il a le statut indéterminé. Dans ce cas, il est soumis au système de réputation pour déterminer son score de réputation.

4.3.2.4 Les différentes fonctions d'analyse des variables

Ce sont des fonctions d'analyse pour chaque variable fournie par le nœud visiteur. Ces fonctions représentent les métriques permettant de calculer les notes pour chaque variable publiée par le nœud visiteur. Le calcul se fait en vérifiant que les variables publiées par le nœud visiteur concordent avec les paramètres attendus par le nœud hôte noté nh. À la sortie de chaque fonction, une note est retournée à propos de chaque variable. Dans la suite, nous présentons chacune des fonctions d'analyse pour chaque variable publiée par le nœud visiteur noté nv.

Fonction d'analyse de la vitesse

L'une des caractéristiques du comportement d'un nœud est la vitesse avec laquelle il se déplace. Nous considérons qu'un nœud n'ayant aucune intention malicieuse se comportera comme la majorité des nœuds de son environnement, c'est-à-dire qu'il se déplacera à une vitesse moyenne appartenant à l'intervalle de vitesse minimum et maximum définit sur ce tronçon. Pour vérifier la conformité de la vitesse du nœud visiteur, ce dernier est soumis à un test de vérification de sa vitesse moyenne lors de l'initiation de la communication avec l'intervalle de

vitesse minimale et maximale prescrit. Le fait de se déplacer à une vitesse qui n'appartient pas à l'intervalle de vitesse attendue est considéré comme un abus. Ce non-respect mène à une note de 0. Par contre si le nœud respecte les limitations de vitesse, la fonction d'analyse retournera une note de 1 dans le cas du modèle binaire et une note appartenant à l'intervalle [0, 1] dans le cas du modèle flexible. Ces deux modèles seront présentés par la suite. Cette métrique permet d'éviter les attaquants qui se placent au bord de la route ou sur un pont pour collecter des informations sur les nœuds. De fait, sur une autoroute où l'intervalle de vitesse moyenne de déplacement varie de [60 km/h , 100 km/h], un nœud qui tente d'entrer en communication en annonçant une vitesse de 50km/h aura une note nulle. Les limitations de vitesse sur les autoroutes du Québec sont de : vitesse minimale (v_{min}), 60km/h et vitesse maximale (v_{max}), 100km/h. La vitesse annoncée par le véhicule visiteur (v_{nv}) doit respecter la condition suivante: $v_{min} \leq v_{nv} \leq v_{max}$, pour avoir une bonne note dans le cas contraire c'est une mauvaise note qui est attribuée pour la variable vitesse. Pour évaluer cette note, on fixe 2 paramètres v_{min} et v_{max}.

Tableau 4.1:Paramètres et variables de la vitesse

Symbole	**Description**
Paramètre : v_{min}	Vitesse minimale attendue
Paramètre : v_{max}	Vitesse maximale attendue
Variable : v_{nv}	Vitesse annoncée par le nœud visiteur nv

Fonction d'analyse de la position géographique

Certains nœuds, dans le but d'agir de façon malicieuse sur le réseau, ne fournissent pas leur position géographique réelle. Le nœud hôte utilise les équipements tels que : le GPS, les radars et les capteurs embarqués pour déterminer la position géographique d'un nœud qui tente d'entrer en communication avec lui [133]. La fonction d'analyse de la position géographique se charge de corroborer l'information qui a été reçue du nœud visiteur par rapport aux observations qui ont été faites par les équipements embarqués. Si les variables sont satisfaisantes, une bonne note sera attribuée à la variable. Dans le cas où les variables ne sont pas satisfaisantes, c'est une mauvaise

note qui est attribuée à la variable. Dans cette fonction d'analyse, nous nous inspirons des travaux de L. Tian et al. [135], qui considèrent qu'il existe une tolérance vis-à-vis des coordonnées réelles d'une voiture. Pour cette raison, dans [133] Yan Gongjun et al. ont proposé une équation que nous reprenons dans nos travaux pour détecter les nœuds qui diffusent une position géographique erronée en évaluant l'inégalité suivante :

$$(x_{nv} - x_a)^2 + (y_{nv} - y_a)^2 \leq (\Delta)^2$$

Tableau 4.2: Paramètres et variables de la position géographique

Symbole	**Description**
Variable: x_a	Valeur de l'abscisse attendue par le nœud hôte nh
Variable: y_a	Valeur de l'ordonnée attendue par le nœud hôte nh
Paramètre : Δ	Facteur de tolérance causé par la distorsion des signaux dans la troposphère et l'ionosphère.
Variable : x_{nv}	Valeur de l'abscisse publiée par le nœud visiteur nv
Variable: y_{nv}	Valeur de l'ordonnée publiée par le nœud visiteur nv

Δ est souvent égal à 10 m. Ce qui nous laisse donc une marge d'erreur de 10 mètres.

Fonction d'analyse des dimensions du véhicule

Les dimensions des véhicules dépendent de la gamme dont ils font partie. Ces dimensions sont connues et sont confinées dans un intervalle connu. Il serait donc curieux qu'un nœud indique des dimensions qui ne sont pas dans un certain intervalle. À moins que ce soit un type de véhicule particulier tel que des gros porteurs ou encore des limousines. Si un véhicule « normal » indique des dimensions qui ne respectent pas les paramètres attendues, la note pour ses variables

de dimension sera mauvaise. Dans le cas où les paramètres attendus sont respectés, la note de ces variables sera bonne. L'inégalité qui permet de construire cette métrique est la suivante :

$$\begin{cases} l_{min} \leq l_{nv} \leq l_{max} \\ L_{min} \leq L_{nv} \leq L_{max} \end{cases}$$

Tableau 4.3: Paramètres et variables des dimensions du véhicule

Symbole	**Description**
Paramètre : l_{min}	Largeur minimale attendue par le nœud hôte
Paramètre :l_{max}	Largeur maximale attendue par le nœud hôte
Paramètre :L_{min}	longueur minimale attendue par le nœud hôte
Paramètre :L_{max}	longueur maximale attendue par le nœud hôte
Variable :l_{nv}	Largeur publiée par le nœud visiteur nv
Variable : L_{nv}	Longueur publiée par le nœud visiteur nv

La fonction d'analyse de la direction

Un véhicule peut circuler dans deux directions possibles : dans la même direction que le nœud hôte est représentée par la valeur 1 ou encore en direction contraire à celle du nœud hôte, est représentée par la valeur -1. En fait dans un contexte de cellule, la direction du nœud hôte est celle vers le centre de la cellule à laquelle appartient le nœud hôte alors que la direction contraire est celle des nœuds qui s'éloignent du centre de la cellule. Grâce aux radars embarqués sur le nœud hôte, celui-ci est capable de déterminer la direction du nœud qui tente de rentrer en communication avec lui. Si la direction publiée par le nœud visiteur coïncide avec la direction attendue, une bonne note est retournée par la fonction d'analyse de la direction. Dans le cas contraire, c'est une mauvaise note qui est retournée. Soit D_{nv} la direction annoncée par le véhicule visiteur et D_a la direction attendue, la métrique permettant de réaliser le test est représentée par l'égalité suivante : D_{nv} - $D_a = 0$.

Tableau 4.4: Paramètres et variables de la direction

Symbole	**Description**
Paramètre : D_a	Direction attendue par le nœud hôte
Variable : D_{nv}	Direction publiée par le nœud visiteur

La fonction d'analyse du rayon de transmission

Chaque véhicule dispose d'une antenne de communication qui définit à quel rayon il peut émettre. Lors de la réception d'une trame beacon provenant du nœud visiteur, le nœud hôte via sa fonction d'analyse du rayon de transmission vérifie que le nœud visiteur ne transmet pas à un rayon supérieur au rayon de transmission légal. Cette métrique permet aussi de vérifier qu'un nœud ne ment pas sur sa position. Ainsi, la note attribuée à cette variable sera bonne si le nœud visiteur transmet à l'intérieur du rayon de transmission. S'il transmet à l'extérieur du rayon de transmission légale, c'est une mauvaise note qui est attribuée à la variable du rayon de transmission. Cette métrique permet d'évaluer si le nœud se trouve à l'intérieur de la cellule. Le rayon de transmission doit être inférieur au diamètre de la cellule. Ainsi l'inégalité utilisée pour vérifier cette métrique est la suivante : $r_{nv} \leq D_a$.

Tableau 4.5: Paramètres et variables du rayon de transmission

Symbole	**Description**
Paramètre : D_a	Diamètre de la cellule dans laquelle se trouve le nœud hôte
Variable r_{nv}	Rayon de transmission publié par le nœud visiteur

La fonction d'analyse de la fréquence de transmission

Une attaque de déni de service consiste souvent pour un nœud à transmettre plusieurs requêtes à une fréquence très élevée de façon à saturer le nœud récepteur. Pour éviter ce type d'attaque, la fonction d'analyse de la fréquence de transmission vérifie la fréquence à laquelle les paquets provenant du nœud visiteur sont envoyés. Si celle-ci est conforme à la fréquence attendue, la fonction retourne une bonne note. Dans le cas contraire, c'est une mauvaise note qui est retournée par la fonction d'analyse. La métrique qui permet de réaliser ce test est définit par l'inégalité suivante : $f_{nv} \leq f_a$.

La fonction d'analyse de l'accélération

L'accélération d'un nœud dépend de sa vitesse, celle-ci doit donc concorder avec la vitesse moyenne sur la chaussée, et ceci à un instant donné. Si le nœud ne respecte pas l'accélération normale qu'il devrait avoir, la fonction d'analyse de l'accélération retournera une mauvaise note, Si par contre la valeur de l'accélération concorde avec celle attendue par le nœud hôte c'est une bonne note qui est attribuée à la variable. La métrique permettant d'obtenir cette note est donnée par l'inégalité suivante : $acc_{min} \leq acc_{nv} \leq acc_{max}$.

Tableau 4.6: Paramètres et variables de l'accélération

Symbole	**Description**
Paramètre : acc_{min}	accélération maximale attendue par le nœud hôte
Paramètre : acc_{max}	accélération minimale attendue par le nœud hôte
Variable acc_{nv}	Accélération publiée par le nœud visiteur

Dans la partie suivante, nous présentons les autres modules qui constituent le système de réputation. Il s'agit du module d'agrégation de la réputation locale, du module d'agrégation de la

réputation locale et indirecte, du module de prise en compte de l'historique et du module de prise de décision.

4.3.3 Le module d'agrégation de réputation locale

Ce module a pour rôle d'additionner l'ensemble des notes obtenues par les différentes variables traitées dans la partie précédente pour former le score local de réputation. Ce score représente le score de réputation du nœud hôte à propos du nœud visiteur sans l'intégration des témoignages des voisins.

4.3.4 Le module d'agrégation de réputation locale et indirecte

Ce module réalise la moyenne de toutes les réputations indirectes fournies par les nœuds voisins concernés. Une fois le score de réputation moyen des voisins à propos du nœud visiteur obtenus, la moyenne de ce score avec le score local de réputation est calculé. La nouvelle moyenne trouvée représente le score de réputation global qui permettra de prendre la décision. Le score de réputation global représente le score de réputation obtenu par le nœud hôte à propos du nœud visiteur, après avoir pris en compte les témoignages des nœuds voisins à propos du nœud visiteur.

4.3.5 La gestion de l'historique d'un nœud

Tout nœud ayant conservé un score de réputation acceptable peut conserver sa place dans la liste des voisins tant que l'âge de son score ne dépasse par un âge seuil défini. Par contre l'historique devient intéressant lorsqu'il faut réhabiliter un nœud qui a précédemment été malicieux et qui est maintenant honnête. Dans ce cas il doit passer par un processus de réhabilitation. Il est donc possible en ce moment-là de lier sa réhabilitation à ses scores précédents avant de le réhabiliter. C'est aussi ce module qui permet de mesurer l'âge des scores de réputation du nœud hôte à propos du nœud voisin.

4.3.6 Le module de prise de décision

Ce module récupère le score de réputation global et le soumet à une analyse qui permet de déterminer le statut qui sera donné au nœud visiteur en question. Deux statuts sont envisageables : si le nœud est considéré comme honnête, la communication est acceptée et le

nœud visiteur devient un voisin. Par contre si le nœud est considéré comme malicieux, la communication est refusée et le nœud visiteur est éjecté du réseau.

4.4 Fonctionnement des modules du système

Dans cette partie, nous présentons dans un premier temps la manière donc les modules du système de réputation fonctionnent, ensuite, nous présentons comment se fait le choix des procédures de calcul des scores de réputation, et enfin nous présentons comment se fait la prise de décision. Nous considérons deux modèles : le modèle binaire qui est rigide non flexible et le modèle flexible qui est souple et qui permet une certaine marge d'erreur.

La terminologie des éléments et des termes adoptés dans notre système est définie dans le tableau ci-dessous.

Tableau 4.7: Description des symboles utilisés dans le système

Symbole	**Description**
M	Ensemble des variables
H	Ensemble des nœuds hôtes
V	Ensemble des nœuds visiteurs
O_{nv}	Ensemble des nœuds voisins des nœuds visiteurs
nh	nœud hôte, $\forall\ nh \in H$
nv	nœud visiteur, $\forall\ nv \in V$
no	nœud voisin, $\forall\ no \in O_{nv}$
r_i	note de la variable i calculée par la fonction d'analyse, $\forall\ i \in M$
δ	Pas utilisé pour définir les notes des variables,

	avec δ ϵ [0,1]
$rl_{nh}(nv)$	score de réputation local du nœud visiteur nv par rapport au nœud hôte nh
ro	score de réputation du nœud visiteur par rapport à l'ensemble des voisins O_{nv}
$rg_i(nv)$	score de réputation global du nœud visiteur par rapport à un nœud voisin
$rg_{nh}(nv)$	score de réputation global du nœud visiteur nv par rapport au nœud hôte nh
$rg_{nh}(no)$	score de réputation global du nœud voisin no par rapport au nœud hôte nh
rp	C'est le score de réputation le plus élevé que peut obtenir un nœud (score de réputation parfait)
T	Âge d'une information courante
$Tmax$	Âge limite supérieur
p	Pourcentage appliqué au score de réputation parfait pour obtenir un seuil
η	Pourcentage appliqué à l'âge limite pour obtenir un seuil

4.5 Le modèle binaire

Dans cette version, les notes ont des valeurs égales à 1 lorsqu'il y a concordance entre le paramètre attendu et la variable publiée. Dans le cas où les paramètres attendus ne sont pas respectés, la note attribuée est égale à 0. Dans ce type de modèle, il n'y a pas de marge d'erreur.

4.5.1 Le calcul de la note pour chaque variable

Il s'agit de la note donnée à une variable particulière. Cette note est binaire et peut donc prendre deux valeurs soit 0, soit 1 selon que les paramètres attendues sont respectés ou pas. Elle est déterminée selon les conditions suivantes pour chaque variable.

Si $val_{min} \leq val_{nv} \leq val_{max}$ alors une note r_i est attribuée, avec r_i=1.

Par contre si $val_{nv} < val_{min}$ ou $val_{nv} > val_{max}$ alors une note r_i est attribuée, avec r_i =0.

Tableau 4.8: Paramètres et des variables d'une variable publiée par le nœud visiteur

Symbole	**Description**
Paramètre : val_{min}	paramètre minimal attendu pour la variable testée
Paramètre : val_{max}	paramètre maximal attendu pour la variable testée
Variable val_{nv}	variable publiée par le nœud visiteur

4.5.2 Le calcul du score local de réputation du nœud visiteur par rapport au nœud hôte

Après avoir récolté les notes pour chaque variable soumise au système de réputation, il faut calculer le score de réputation local. Ce score est calculé en faisant la somme de tous les scores de réputation brute. Ce qui est donné par la formule suivante :

$rl_{nh}(nv) = \sum r_i$, avec $i \in M$ (1)

4.5.3 Score global de réputation

Le score de réputation global représente l'agrégation des scores locaux de réputation et les témoignages des voisins.

4.5.3.1 Prise en compte des témoignages des voisins

Les scores fournis par les voisins (que nous appelons aussi témoignages ou score de réputation indirecte) à propos du nœud visiteur sont pris en considération s'ils sont encore valables, c'est-à-dire que l'âge de ces scores est inférieur ou égal à l'âge limite défini. L'âge limite à respecter est représenté par $Tmax$. Dans le cas contraire, l'information publiée par ce voisin n'est pas pris en considération. L'algorithme permettant de réaliser cette opération est le suivant : On parcourt la liste des voisins et pour chaque voisin, on teste l'âge du témoignage, si cet âge est encore valide, alors on prend en considération le témoignage $ro(nv)$ du nœud visiteur par rapport aux nœuds voisins.

Le score de réputation global du nœud visiteur par rapport aux nœuds voisins est donné par :

$$ro(nv) = \frac{1}{|O_{nv}|} \sum rg_i(nv) \quad \text{, avec } i \in O_{nv} \tag{2}$$

4.5.3.2 Calcul du score global de réputation

Le score global de réputation du nœud visiteur par rapport au nœud hôte est déterminé en réalisant la moyenne du score local de réputation du nœud visiteur par rapport au nœud hôte et le score global de réputation du nœud visiteur par rapport aux nœuds voisins. C'est ce score global de réputation qui est soumis au module de prise de décision. La formule permettant de calculer le score global de réputation est la suivante :

$$rg_{nh}(nv) = \frac{1}{2}\left(rl_{nh}(nv) + ro(nv)\right) \tag{3}$$

4.5.4 Le module de prise de décision

C'est le module de prise de décision qui détermine si le nœud est accepté donc ajouté à la liste des voisins ou alors rejeté c'est-à-dire ajouté dans la liste noire. Le nœud est accepté si son score global de réputation est supérieur à un seuil d'acceptation fixé. La procédure permettant de prendre la décision est donnée par l'inégalité suivante : si

$rg_{nh}(nv)$ >=p× rp alors la communication est acceptée, sinon, la communication est refusée. Avec p le poids associé au score parfait de réputation rp.

4.6 Modèle flexible

Le modèle flexible diffère du modèle binaire en trois principaux points :

- Les notes des variables ne sont plus binaires mais peuvent prendre une valeur δ intermédiaire entre 0 et 1. δ ϵ [0, 1].
- Une procédure de réhabilitation est introduite. Cette procédure permet d'accepter un nœud qui était considéré comme malicieux dans des communications précédentes et qui se comporte maintenant de façon exemplaire. Par contre il devra être observé pendant une certaine durée et il devra maintenir un score de réputation acceptable pendant toutes les tentatives de communication durant cette période. Il ne pourra avoir le statut de nœud honnête que s'il respecte les conditions précédemment citées.
- Les témoignages des voisins sont maintenant soumis à une contrainte supplémentaire, en plus de l'âge des scores. Il s'agit de son score de réputation par rapport au nœud hôte. Ce score doit être supérieur à un seuil préalablement fixé. Cette nouvelle contrainte a pour but de filtrer les témoignages donnés par les nœuds voisins, afin d'éviter des témoignages fallacieux.

Ces nouvelles considérations introduisent plus de flexibilité à notre système de réputation. La réhabilitation impose l'introduction de deux nouvelles listes :

La liste de réhabilitation : elle stocke les identifiants des nœuds qui sont en cours de réhabilitation. Ce sont des nœuds qui étaient considérés comme malicieux et qui ont maintenant des scores acceptables de réputation. Avant d'être accepté, ils passent par un processus de réhabilitation. Ce processus se présente de la façon suivante : Dans le cas où le nœud visiteur faisait partie de la liste noire et que son score de réputation est maintenant acceptable, on le met dans un processus de réhabilitation. Ce processus consiste à observer le comportement d'un nœud dans les n dernières périodes de communication, De ce fait, on insère dans une liste de réhabilitation ses scores de réputation des précédentes périodes, s'il a maintenu un score de réputation acceptable, il est réhabilité et est intégré dans la liste des voisins. S'il n'a pas maintenu un score de réputation acceptable dans les n dernières périodes successives, il est totalement éjecté du réseau et son identifiant est inséré dans la liste rouge; n ϵ N et est défini lors de

l'implémentation du système. C'est le processus de réhabilitation qui met en exergue le concept d'historique du nœud. En effet, un nœud ayant toujours conservé un score de réputation acceptable conservera toujours sa place dans la liste des voisins. Par contre l'historique d'un nœud devient important lorsqu'il faut le réhabiliter parce qu'il a précédemment été malicieux et qu'il est maintenant honnête. Dans ce cas, il doit passer par un processus de réhabilitation. Il est donc possible en ce moment-là de lier sa réhabilitation à ses scores de réputation précédents avant de le réhabiliter.

La liste rouge : elle stocke les identifiants des nœuds qui ont été considérés comme malicieux et ne peuvent plus bénéficier d'une réhabilitation. Ils sont bannis du réseau.

4.6.1 Le calcul de la note pour chaque variable

La note attribuée à chaque variable comme nous l'avons mentionné plus haut, est défini en considérant un pourcentage δ dans l'intervalle [0, 1]. Les inégalités qui permettent de noter les variables sont données dans la partie suivante :

- Si val_{min} <= val_{nv} <= val_{max} alors r_i = 1
- Si val_{nv} < δ ×val_{min} ou val_{nv} > (1 + (1- δ)) × val_{max} alors r_i = 0

Pour relâcher les contraintes, on peut décider d'accepter des variables qui ne sont pas dans l'intervalle attendu, mais qui ont une valeur inférieure à la valeur minimale attendue. On aura alors la relation suivante :

- Si δ ×val_{min} <= val_{nv} < val_{min} alors r_i = δ et r_i ϵ [0, 1].

De la même façon, on peut accepter des valeurs qui sont supérieures à la valeur maximale attendue. L'inégalité suivante présente ce cas de figure :

- Si val_{max} < val_{nv} <= (1 + (1- δ)) × val_{max} alors r_i = δ , ∀ r_i ϵ [0, 1], $i \in M$.

Ces inégalités prennent en considération la possibilité d'une marge d'erreur dans les valeurs fournies par les variables.

4.6.2 Le calcul des scores de réputation

Le score de réputation local pour le modèle flexible se calcule de la même façon que pour le modèle binaire.

Le score de réputation globale se calcule aussi de la même façon que pour le modèle binaire à la différence que le témoignage des voisins est soumis à de nouvelles contraintes qui impliquent un bon score de réputation passé et qui est assez jeune.

4.6.3 Prise en compte des témoignages des voisins

Les témoignages fournis par les voisins à propos du nœud visiteur sont pris en considération selon les conditions suivantes :

- Le nœud voisin en question, lors de ses derniers échanges avec le nœud hôte doit avoir obtenu un score de réputation supérieur au seuil p×rp et le témoignage publié doit être âgé d'au plus η×$Tmax$ pour être pris en compte. Si ces conditions ne sont pas respectées, alors le témoignage du voisin sur le nœud visiteur n'est pas considéré.

Pour chaque voisin, les conditions suivantes doivent donc être respectées : si $rg_{nh}(no) \geq$ p×rp ET $T \leq$ η×$Tmax$ alors on applique au témoignage du voisin un poids α_i tel que $rg_i(nv) = \alpha_i \times rg_i(nv)$ avec $\alpha_i \in [0, 1]$, ensuite les mêmes formules que pour le modèle binaire sont utilisées pour calculer le score de réputation du nœud visiteur par rapport à tous les voisins sélectionnés. Une fois que le témoignage des voisins est déterminé et que le score de réputation global est calculé alors la décision est prise. Plusieurs cas régissent cette prise de décision.

4.6.4 Les différents cas régissant la prise de décision

Le système de réputation du nœud hôte prend sa décision à propos du nœud visiteur en considérant le statut définit pour ce dernier dans le module de vérification de l'identité. Les cas suivants sont envisageables :

Cas 1 : nœud visiteur avec statut indéterminé

Le nœud visiteur est nouveau dans le réseau, dans ce cas, c'est le score de réputation local qui sera considéré pour la prise de décision. Si la contrainte sur le score est respectée alors le nœud est accepté et il est ajouté dans la liste des voisins, sinon le nœud est rejeté et il est alors ajouté dans la liste noire.

Cas 2 : nœud visiteur ayant été voisin

Dans le cas où le nœud visiteur fait partie de la liste des voisins, son score de réputation globale est vérifié. Si le score de réputation n'est pas acceptable, le nœud est éjecté et ajouté dans la liste noire. Si ce score est acceptable, son historique est vérifié, si l'âge des informations est inférieur à l'âge limite fixé, le nœud est accepté pour communiquer avec le nœud hôte, sinon il est éjecté.

Cas 3 : nœud visiteur de la liste noire

Si le nœud visiteur existait déjà dans la liste noire, on vérifie son score de réputation pour savoir si celui-ci est maintenant acceptable. Si c'est le cas, il est ajouté dans la liste de réhabilitation. Si ce n'est pas le cas, il est conservé dans la liste noire et la communication est refusée.

Cas 4 : nœud visiteur dans la liste de réhabilitation

Si le nœud fait partie de la liste de réhabilitation, son historique est vérifiée, s'il a conservé un score de réputation acceptable pendant un nombre défini de tentative de communications et dans un temps acceptable, alors il est accepté et ajouté dans la liste des voisins. Sinon il est banni et envoyé dans la liste rouge.

4.6.5 Le module de prise de décision

C'est le module de prise de décision qui détermine si le nœud visiteur est accepté, rejeté ou banni. À la suite de cette décision, l'identifiant du nœud est ajouté dans l'une des listes citées plus haut. Si le nœud est honnête, il est ajouté dans la liste des voisins, s'il est malicieux, il est ajouté dans la liste noire et enfin s'il est banni, il est ajouté dans la liste rouge. La procédure représentant la prise de décision est donnée par l'inégalité suivante : Si $rg_{nh}(nv)$ >= p×rp alors la communication est acceptée sinon la communication est refusée.

4.7 Définitions mathématiques du système de réputation

4.7.1 Présentation

Dans cette partie, nous présentons les formules mathématiques qui ont permis de calculer les notes attribuées aux différentes variables, les scores locaux et globaux de réputation pour notre système SSVR. La définition mathématique que nous présentons, s'inspire des travaux effectués par Michiardi et Molva dans [128]. La nomenclature est la même que celle présentée dans le tableau 4.7.

4.7.2 Note pour chaque variable

Il s'agit de la note qui est attribuée à chaque variable :

$r_{nh}(nv|i) = p_i \times r_i$, avec $i \in M$ et p_i : poids lié à la note r_i , $p_i \in [0, 1]$ (1)

4.7.3 Score local de réputation du nœud visiteur par rapport au nœud hôte

Le score local de réputation est donné par la somme des notes attribuées à chaque variable. La formule mathématique liée à ce score est la suivante :

$r_{nh}(nv) = \sum_i p_i \times r_i = \sum_i r_{nh}(nv|i)$, avec $i \in M$, p_i : poids lié à la note r_i , $p_i \in [0, 1]$ (2)

4.7.4 Score indirect de réputation

Il s'agit du score de réputation du nœud visiteurs par rapport aux voisins. Il est donné par la formule :

$ro(nv) = \frac{1}{|O_{nv}|} \sum p_{no} \times r_{no}(nv)$, avec $no \in O_{nv}$, p_{no}: Poids lié au témoignage du nœud voisin, $p_{no} \in [0, 1]$ (3)

4.7.5 Score global de réputation du nœud visiteur par rapport au nœud hôte

Une fois que le score local de réputation est calculé, celui-ci est agrégé aux scores de réputation indirecte afin d'avoir un score global. Cette agrégation se fait par la formule suivante :

$$rg_{n_h}(nv) = \frac{1}{2}\left(r_{nh}(nv) + ro(nv)\right) \quad (4)$$

La modélisation mathématique permet d'avoir une base de définition des différents scores que propose le système de réputation. Celle-ci peut être exploitée dans des contextes différents et peut être modifiée selon les contraintes du système.

4.8 L'algorithme

La majorité des protocoles de communication intègrent des systèmes de sécurité permettant seulement de détecter les nœuds malicieux. Mais ils ne fournissent pas un moyen efficace de les exclure du réseau. C'est la raison pour laquelle nous avons proposé SSVR, un système qui permet de détecter les nœuds malicieux et de les éjecter du réseau ou de les réhabiliter. L'algorithme sur lequel se base notre système est présenté ci-dessous.

Cet algorithme est constitué d'un ensemble de fonctions qui analysent chacune des variables fournies par le paquet reçu provenant du nœud visiteur qui souhaite entrer en communication avec le nœud hôte. Les informations prises en compte dans chaque fonction ont été présentées dans le tableau 4.7. Cet algorithme agit à l'interface d'entrée du réseau pour chaque nœud lors de la réception de nouvelles demandes de communication. Nous considérons un environnement de réseau Ad-hoc dans lequel chaque nœud souhaitant intégrer le réseau doit diffuser des trames beacon pour découvrir le réseau. Ce sont les informations contenues dans ces trames beacon qui sont analysées. Deux types de paquets sont considérés dans notre système, les paquets de requêtes par lesquels le nœud fait des demandes de communication et les paquets de réponses par lesquels le nœud hôte répond à ces requêtes. L'algorithme représenté dans le tableau 4.10 est utilisé pour évaluer chaque message. Nous considérons comme nous l'avons indiqué dans les sections 4.8 et 4.9, le modèle binaire et le modèle flexible. La terminologie utilisée dans cette section est la même que celle utilisée dans le tableau 4.7. Dans le tableau suivant, nous faisons la description des nouveaux symboles qui n'ont pas été employés dans les sections précédentes.

Tableau 4.9: Description des nouveaux symboles utilisés dans les algorithmes

N	Ensemble des nœuds de la liste noire
R	Ensemble des nœuds de la liste de réhabilitation

U	Ensemble des nœuds de la liste rouge
$m_{nv}(i)$	Message publié par le nœud visiteur, avec $i \in M$
id	Identifiant du nœud
T_{nv}	L'âge du score du nœud visiteur
t	Temps du début de la communication courante
c	nombre de fois où un nœud en réhabilitation a eu un score de réputation acceptable
$t(nv)$)	Temps de début de la dernière communication
r_n	Valeur de réputation attribuée à une variable lorsque l'information ne concorde pas. r_n = 0
r_p	Score de réputation attribué à un nœud lorsque l'information concorde. $r_p \in]0, 1]$

4.8.1 Algorithme du modèle binaire

Dans cette partie, nous présentons l'algorithme du système de réputation SSVR pour le modèle binaire. Il est constitué de plusieurs fonctions qui réalisent chacune une tâche spécifique.

Les différentes fonctions utilisées dans l'algorithme sont présentées dans la suite :

- ProcessMessage ($m_{nv}(id)$) : fonction permettant de tester l'identifiant publié par le nœud visiteur.
- processMessage ($m_{nv}(i)$): fonction qui teste chacune des variables publiées par le nœud visiteur.
- agregatedLocal (r_i): fonction dans laquelle se fait l'agrégation des différentes notes obtenues par les variables publiées par le nœud visiteur.

- integratedNeighbours ($rg_i(nv)$) : fonction ayant pour rôle la prise en compte des témoignages des voisins. Elle retourne le score de réputation pour l'ensemble des voisins.
- computedGloabal ($rl_{nh}(nv)$, ro) : fonction qui permet de faire le calcul du score de réputation global qui sera utilisé pour la prise de décision.
- checkTime (T_{nv}): fonction ayant pour tâche de vérifier si l'âge d'une information est inférieur à un âge limite fixé
- rejected (nv): fonction qui éjecte du réseau un nœud visiteur défini comme malicieux.
- Accepted (nv): fonction qui accepte un nœud visiteur dans le réseau.
- decisionTaken ($rg_{nh}(nv)$) : fonction dans laquelle la décision d'accepter la communication ou d'éjecter le nœud visiteur est prise.

Tableau 4.10: Algorithme du système de réputation SSVR-modèle binaire

```
begin
ProcessMessage (m_nv(id))
If(id ϵ N) then
    rejected(nv)
else if(id ϵ V)
    checkTime(T_nv)
    if(checkTime(T_nv)== true)
          accepted(nv)
     else
         while(i ϵ M)
            processMessage (m_nv(i));
       agregatedLocal (r_i)
       integratedNeighbours (rg_i(nv)) // i ϵ O_nv
       computedGloabal (rl_nh(nv), ro)
```

decisionTaken ($rg_{nh}(nv)$)

else

while(i)

processMessage ($m_{nv}(i)$);

agregatedLocal (r_i)

integratedNeighbours ($rg_i(nv)$) // $i \in O_{nv}$

computedGloabal ($rl_{nh}(nv)$, ro)

decisionTaken ($rg_{nh}(nv)$)

end

processMessage ($m_{nv}(i)$)

if ($m_{nv}(i)$) dans l'intervalle $r_i = 1$

else

$r_i = 0$

agregatedLocal (r_i)

while(i)

$rl_{nh}(nv)$ += r_i

return ($rl_{nh}(nv)$)

integratedNeighbours ($rg_i(nv)$) // $i \in O_{nv}$

while(i) // $i \in O_{nv}$

if(checkTime ($T(rg_i(nv))$== true)

ro += $rg_i(nv)$

return ($\frac{1}{|O_{nv}|} ro$)

computedGlobal ($rl_{nh}(nv), ro$)

if($ro == 0$)

$rg_{nh}(nv) = rl_{nh}(nv)$

else

$rg_{nh}(nv) = \frac{1}{2}(rl_{nh}(nv) + ro)$

return $rg_{nh}(nv)$

decisionTaken ($rg_{nh}(nv)$)

if($rg_{nh}(nv)$) tie in)

accepted(nv)

else

rejected(nv)

Accepted(nv)

V = V∪ nv

rejected(nv)

N = N ∪ nv

4.8.2 Description générale de l'algorithme - modèle binaire

L'algorithme ci-dessus décrit le fonctionnement global du système de réputation que nous proposons. Dans cette partie, nous présentons le modèle binaire. Dans un premier temps, le message reçu d'un hôte visiteur est soumis à un système d'évaluation des messages. Celui-ci vérifie l'identifiant du nœud (ProcessMessage ($m_{nv}(id)$)). Si le nœud fait partie de la liste noire, il est éjecté du réseau. Si par contre le nœud fait partie de la liste des voisins, alors le nœud hôte vérifie la durée séparant cette communication à la dernière communication réalisée avec ce nœud pour vérifier que les informations collectées à propos de ce dernier ne sont pas obsolètes. Si les informations ne sont pas obsolètes, la communication est automatiquement acceptée. Mais s'il s'avère que les informations sont obsolètes c'est-à-dire que l'âge acceptable pour la validité du

dernier score de réputation du nœud visiteur par rapport au nœud hôte est dépassé, alors le nœud visiteur est de nouveau soumis aux différentes fonctions d'analyse des variables. Si le nœud visiteur ne fait partie au préalable d'aucune liste, alors c'est un nouveau nœud dans le réseau. Il est donc soumis aux fonctions d'analyses. Ensuite, la réputation globale est déterminée et une décision est prise.

4.8.2.1 Le processus de vérification

Ce processus représente le second niveau du système de réputation. Il est constitué de :

Fonctions d'analyse des variables (processMessage ($m_{nv}(i)$)) : Ces fonctions analysent chaque variable et vérifient si cette dernière concorde avec les informations attendues. Si c'est le cas, une note de 1 est attribué pour cette variable, si ce n'est pas le cas, c'est plutôt une note nulle qui est attribuée. Toutes les variables présentées dans la section 4.3 sont soumises à ce processus et chaque fonction d'analyse traite une variable particulière. Une fois des notes des variables récoltées, elles sont envoyées au module d'agrégation des scores en local.

Module d'agrégation des scores en local (agregatedLocal (r_i)): Ce module a pour principale tâche de faire la somme des notes obtenues par chaque fonction d'analyse. C'est cette somme qui représente le score de réputation local. A la suite de l'obtention du score local de réputation, le système recherche les scores indirects de réputation provenant du voisinage.

Module de prise en compte des scores indirects (integratedNeighbours ($rg_i(nv)$)): Les scores indirects de réputation, appelés aussi témoignage représentent les scores de réputation collectés par les nœuds voisins lorsque ceux-ci ont communiqué avec le nœud visiteur. Chacun des nœuds ayant communiqué avec le nœud voisin depuis un temps acceptable fourni le score de réputation obtenu lors de la dernière communication. Tous ces scores sont additionnés et le résultat de cette somme est ensuite divisé par le nombre de nœuds voisins ayant participé à ce témoignage. Le résultat obtenu constitue le score indirect de réputation, c'est ce score qui sera additionné au score local de réputation pour obtenir le score global de réputation.

Module de réputation global (computedGlobal($rl_{nh}(nv), ro$)) : Ce module a pour rôle d'agréger le score local de réputation au score indirect de réputation, pour ce faire, les deux scores de réputation sont sommés ensuite le résultat obtenu est divisé par deux. C'est la valeur obtenue à la suite des différents calculs qui représente le score global de réputation. Dans le cas

ou le score indirect de réputation n'est pas disponible, c'est le score local de réputation qui est utilisé en lieu et place de score global de réputation. C'est ce score dernier score qui permet de réaliser la prise de décision.

Module de prise de décision (decisionTaken ($rg_{nh}(nv)$)) : C'est dans ce module que la décision est prise, à savoir si le nœud visiteur est accepté ou éjecté du réseau. Cette décision est prise en considérant le score global de réputation obtenu par le nœud hôte à propos du nœud visiteur. Le score global de réputation doit atteindre un pourcentage préalablement définit du score de réputation parfait. Si le pourcentage recherché est atteint, alors le nœud est accepté, il est ajouté dans la liste des voisins s'il n'y existait pas déjà. Dans le cas ou le pourcentage recherché n'est pas atteint, alors le nœud est éjecté (rejected(nv)) du réseau et ajouté dans la liste noire s'il n'y était pas déjà.

4.9 Algorithme du modèle flexible

Cet algorithme reprend les mêmes fonctions que le modèle flexible. Il intègre en plus la fonction de réhabilitation rehabilitated (nv).

Tableau 4.11: Algorithme du système de réputation SSVR-modèle flexible

begin

processMessage ($m_{nv}(id)$)

If(id ϵ N) then

while(i)

processMessage ($m_{nv}(i)$)

agregatedLocal (r_i)

integratedNeighbours ($rg_i(nv)$) // $i \epsilon O_{nv}$

computedGloabal ($rl_{nh}(nv), ro$)

decisionTaken ($rg_{nh}(nv)$)

else if (id ϵ V)

checkTime ($t(nv)$)

if (checkTime ($t(nv)$) == true)

accepted (nv)

else

while(i)

processMessage ($m_{nv}(i)$)

agregatedLocal (r_i)

integratedNeighbours ($rg_i(nv)$) // $i \in O_{nv}$

computedGloabal ($rl_{nh}(nv), ro$)

decisionTaken ($rg_{nh}(nv)$)

else

while(i)

processMessage ($m_{nv}(i)$)

agregatedLocal (r_i)

integratedNeighbours ($rg_i(nv)$) // $i \in O_{nv}$

computedGloabal ($rl_{nh}(nv), ro$)

decisionTaken ($rg_{nh}(nv)$)

end

processMessage ($m_{nv}(i)$)

if ($m_{nv}(i)$) tie in)

$r_i = r_p$ //$r_p \in]0, 1]$

else

$r_i = r_n$ // $r_n = 0$

agregatedLocal (r_i)

while(i)

$rl_{nh}(nv)$ += r_i

Return ($rl_{nh}(nv)$)

integratedNeighbours ($rg_i(nv)$) // $i \in O_{nv}$

while(i) // $i \in O_{nv}$

if (($rg_{nh}(no) \geq p \times r_p$) AND (checkTime ($T(rg_i(nv))$== true))

ro += $q \times rg_i(nv)$

Return ($\frac{1}{|O_{nv}|} ro$)

Else

Return;

computedGloabal($rl_{nh}(nv), ro$)

if($ro == 0$)

$rg_{nh}(nv)$ = $rl_{nh}(nv)$

else

$rg_{nh}(nv)$ = $\frac{1}{2}(rl_{nh}(nv) + ro)$

Return $rg_{nh}(nv)$

decisionTaken ($rg_{nh}(nv)$)

if ($id \in$ N)

if($rg_{nh}(nv)$) tie in)

rehabilitated (nv)

else

rejected(nv)

else

if($rg_{nh}(nv)$) tie in)

accepted(nv)

else

rejected(nv)

Accepted(nv)

V = V ∪ nv

rejected(nv)

N = N ∪ nv

Rehabilitated (nv)

U = U ∪ nv

setTime (t)

c = c + 1

checkTime ($t(nv)$)

if ($t(nv) \leq \eta \times T_{max}$)

return true

else

return false;

setTime (t)

$t(nv)$ = t

4.9.1 Description générale de l'algorithme – modèle flexible

Le modèle flexible reprend globalement le modèle binaire en y ajoutant de la flexibilité. Nous allons présenter les différentes parties de l'algorithme en insistant sur les spécificités de ce modèle. Comme dans le cas du modèle binaire, le message reçu d'un hôte visiteur est soumis à un système d'évaluation des messages. Celui-ci vérifie l'identifiant du nœud si le nœud fait partie de la liste noire, il n'est pas automatiquement éjecté du réseau comme pour le modèle binaire, il est plutôt soumis au système de réhabilitation afin de déterminer s'il est maintenant honnête. Si par contre le nœud fait partie de la liste des voisins, alors le système vérifie la durée séparant cette communication à la dernière communication réalisée avec ce nœud pour vérifier que les informations collectées à propos de ce dernier ne sont pas obsolètes. Si les informations ne sont pas obsolètes, la communication est automatiquement acceptée. Mais s'il s'avère que les informations sont obsolètes c'est-à-dire que l'âge acceptable pour la validité du dernier score de réputation est dépassé, alors le nœud est de nouveau soumis au processus de vérification. Cette partie se déroule comme pour le modèle binaire. Si le nœud ne fait partie au préalable d'aucune liste, alors c'est un nouveau nœud dans le réseau. Il est donc soumis au processus de vérification. Au bout du processus de vérification, un score global de réputation est déterminé et une décision est prise.

4.9.2 Le processus de vérification

Ce processus représente le second niveau du système de réputation. Il est constitué de :

Fonctions d'analyse des variables (processMessage ($m_{nv}(i)$)): Ces fonctions analysent chaque variable et vérifient si cette dernière concorde avec les paramètres attendus. La différence avec le modèle binaire est perceptible à ce niveau, car s'il y a concordance, la note attribuée peut prendre une valeur comprise dans l'intervalle [0,1], s'il n'y a pas concordance, c'est plutôt un score nul qui est attribué. Toutes les variables présentées dans la section 4.3 sont soumises à ce processus de vérification et chaque fonction d'analyse traite une variable particulière. Une fois que l'ensemble des notes des différentes variables est récolté, elles sont envoyées au module d'agrégation des scores en local.

Module d'agrégation des scores en local (agregatedLocal (r_i)): Ce module, comme dans le cas du modèle binaire a pour principale tâche de faire la somme des notes de variables obtenues

par chaque fonction d'analyse. C'est la somme de ces notes qui représente le score local de réputation. A la suite de l'obtention du score local de réputation, le système recherche les scores indirects de réputation.

Module de prise en compte des scores indirects de réputation (integratedNeighbours ($rg_i(nv)$)): Les scores indirects de réputation, appelé aussi témoignage représentent les scores de réputation collectés par les nœuds voisins lorsque ceux-ci ont communiqué avec le nœud visiteur. Chacun des nœuds ayant communiqué avec le nœud voisin depuis un temps acceptable fourni le score de réputation obtenu lors de la dernière communication. Contrairement au modèle binaire, cette contrainte n'est pas la seule, le score de réputation obtenu par le nœud hôte à propos du nœud voisin doit aussi être supérieur à un pourcentage du score de réputation parfait (c'est le meilleur score possible), pour que ses témoignages soient pris en compte. Tous les témoignages récoltés sont additionnés et le résultat de cette somme est ensuite divisé par le nombre de nœuds voisins ayant participé à ce témoignage. Le résultat obtenu constitue le score indirect de réputation, c'est ce score qui sera additionné au score local de réputation pour obtenir le score global de réputation.

Module de réputation globale computedGloabal ($rl_{nh}(nv), ro$): Ce module a pour rôle d'agréger le score local de réputation au score indirect de réputation, il fonctionne exactement de la même façon que dans le modèle binaire.

Module de prise de décision (decisionTaken ($rg_{nh}(nv)$)): Ce module fonctionne de la même façon que pour le modèle binaire à la différence qu'un nœud qui était dans la liste noire avant et qui est maintenant honnête sera soumis à un processus de réhabilitation. Il devra demeurer honnête pendant une certaine durée et un certain nombre de tentative de communication avant d'être finalement accepté parmi les voisins.

Module de réhabilitation (Rehabilitated (nv)**)** : Il a pour rôle principal de gérer la liste de réhabilitation. Tout nœud précédemment malicieux qui a un score de réputation acceptable est ajouté à la liste de réhabilitation. Un compteur est mis-à-jour pour compter le nombre de fois successif où le nœud a un score acceptable. Un gestionnaire de temps est aussi mis en place pour constater l'obsolescence des informations. Ainsi la condition de réhabilitation est que le nœud maintienne un score acceptable pendant un certain nombre de fois et pendant une durée définie.

Dans cette section, nous avons présenté deux versions de l'algorithme du système de réputation SSVR. Les deux algorithmes ont plusieurs aspects en commun, la différence fondamentale réside dans la prise en compte des témoignages, en effet pour que les témoignages d'un voisin soit accepté dans le modèle flexible, il faut que celui-ci ait eu une note qui permette au nœud hôte d'avoir une grande confiance à son témoignage. Les autres différences résident d'une part dans la possibilité de réhabilitation d'un nœud qui a été malicieux par le passé. Dans le modèle flexible, les notes attribuées aux variables ne sont plus binaires, ils peuvent prendre plusieurs valeurs intermédiaires entre 0 et 1. Ces changements réalisés dans le modèle flexible du système de réputation le rendent plus robuste et plus flexible.

CHAPITRE 5

EVALUATION DES PERFORMANCES DU SYSTÈME

Dans cette partie, nous allons réaliser des simulations pour tester notre système de réputation. Pour ce faire, nous choisissons un type d'attaque particulier pour lequel notre système est particulièrement efficace. Il s'agit de l'attaque d'illusion car c'est une attaque dont le principal but est de fournir des informations erronées aux nœuds voisins afin de modifier le comportement des automobilistes. Nous avons choisi de réaliser nos simulations en considérant l'application d'avertissement coopérative de collision. Dans la suite, nous allons dans un premier temps présenter l'attaque d'illusion, ensuite, nous présentons l'application d'avertissement coopérative de collision et enfin nous réalisons nos scénarios de simulation et nous analysons les résultats obtenus.

5.1 L'attaque d'illusion

L'attaque d'illusion consiste pour un adversaire, de trafiquer intentionnellement ses équipements de collectes d'informations (senseurs, antenne de communication, etc.) afin de diffuser de fausses informations dans son voisinage [74]. La diffusion de ces informations erronées donne l'illusion d'une situation normale. Par ce processus, l'adversaire peut induire en erreur les automobilistes voisins avec lesquels il communique. Cette situation peut conduire à des accidents ou causer du trafic sur la route. Car le comportement des automobilistes peut fortement dépendre des messages qu'ils reçoivent. L'attaque d'illusion peut être définie comme une attaque qui mène au changement de comportement d'un conducteur par la diffusion de faux messages [136]. Par exemple l'adversaire peut diffuser sur le réseau une fausse alerte d'accident pour faire décélérer ou accélérer ces voisins et même les faire changer de chemin. Il peut aussi lancer un message de freinage brusque, les véhicules qui arrivent voudront ralentir pour ne pas causer de collision. Normalement les automobilistes ne sont pas sensé réagir en se fiant seulement à la réception de messages d'alerte, dans la pratique, ils ont l'intuition de vérifier la situation environnante avant d'agir. Mais dans les conditions particulières telles qu'en période de neige, de pluie ou encore dans la nuit, les automobilistes feront d'avantage confiance aux messages reçus et dans ces conditions une attaque d'illusion est facile à perpétrer. Les adversaires

ayant l'intention de perpétrer une telle attaque ne diffusent pas les informations exactes attendues par le nœud hôte.

Notre système de réputation peut intervenir pour détecter les informations erronées, il effectue des vérifications non pas sur le type de l'information, ou le signal diffusé (message d'alarme d'une collision ou d'un freinage brusque), mais plutôt sur les informations annexes transmises, telles que sa position géographique, sa vitesse, etc. Dans la suite, nous présentons l'application d'avertissement coopératif de collision frontale

5.2 Avertissement coopératif de collision frontale

Les caractéristiques de ce type d'application sont les suivantes [137]: la définition de l'application et la description de l'application.

Définition de l'application

Les messages d'avertissement de collision sont conçus pour aider le conducteur à éviter ou à atténuer une collision avec le véhicule qu'il suit, grâce à des messages d'avertissement envoyés par d'autres véhicules. Le système ne cherche pas à contrôler le véhicule hôte afin d'éviter la collision. Mais c'est l'automobiliste qui doit prendre les actions nécessaire afin d'éviter cette collision, soit en décélérant, soit en changeant de couloir.

Description de l'application

Le système d'avertissement coopératif de collision est une extension du système d'avertissement de collision par les radars. Ce système utilise les informations publiées par les véhicules voisins à travers les communications de véhicule à véhicule. Le véhicule hôte reçoit du véhicule visiteur les informations concernant la position géographique, la direction, l'accélération, etc. En utilisant ces informations et en tenant compte de sa propre position, de sa vitesse actuelle et des informations sur l'état actuel de la route, le véhicule hôte pourra déterminer si une collision avec le véhicule qu'il suit est plausible ou non

Pour l'évaluation des performances de notre système, nous allons considérer un adversaire qui tente de perpétrer une attaque d'illusion en publiant au nœud hôte des informations erronées dans son message d'avertissement coopératif à une collision.

5.3 Les simulations

Dans cette section, nous réalisons différents tests de simulation pour mesurer l'efficacité et évaluer les performances de notre système de réputation.

Nous réalisons nos simulations avec le simulateur NS [138] (Network Simulator), dans sa version 2. C'est un simulateur qui est largement utilisé pour la simulation des réseaux pour les protocoles TCP et IP, des protocoles de routages et d'autres applications dans les réseaux filaires et sans fil.

Nous exploitons le protocole de routage AODV(Ad hoc On Demand Distance Vector), qui est l'un des protocoles de routage utilisé dans les VANETs [139]. En effet trois types de messages sont définis dans le protocole AODV, il s'agit de Route Request RREQs (message de requêtes), Route Replies, RREPs (message de réponse), Route Errors, RERRs (message d'erreur). Pour mener à bien nos simulations, nous modifions l'entête de la requête RREQs dans laquelle nous insérons les différentes variables de notre système (identifiant du nœud, vitesse du nœud, accélération, position géographique, fréquence de transmission, rayon de transmission, dimensions du nœud et direction du nœud). Toutes ces informations seront soumises aux différents tests de notre système. Dans la fonction de réception des messages, nous intégrons notre algorithme de réputation de tel enseigne que chaque message qui est reçu est soumis aux tests de notre algorithme.

Tous les messages RREQs reçus par le nœud hôte sont soumis aux tests de notre algorithme avant d'être traité s'ils sont acceptés dans le réseau. Ainsi, chaque requête contenant des informations erronées dans son entête sera supprimée, les requêtes ayant les bonnes informations seront traitées et une réponse sera envoyée au nœud visiteur ayant soumis les dites requêtes. Le tableau 5.1 présente la configuration de notre système pour la réalisation des simulations avec le logiciel NS-2.

Tableau 5.1: Configuration du système

Paramètres	**Valeurs**
Type de canal	Wireless

Type d'interface réseau	Physical Wireless
Protocol de routage	AODV (NS2 default)
Type d'interface de la queue	Priority queue
Longueur de la queue	50 paquets
Nombre de nœuds dans la topographie	12, 20
Dimension de la topographie en x et y	500*400
Durée de la simulation	150s
Type du trafic	TCP
Vitesse	40m/s
Modèle de propagation radio	Two ray ground
Protocol MAC	IEEE 802.11

5.4 Plan d'expérimentation

Dans cette section, nous présentons les objectifs de notre étude de performance, ensuite, nous présentons les différents modèles de charge : notamment le modèle stochastique et le modèle déterministe.

5.4.1 Objectif de l'étude de performance

Notre objectif dans cette étude de performance est de démontrer que notre système est fonctionnel c'est-à-dire qu'il est capable de détecter des nœuds malicieux. Ensuite nous évaluons l'efficience de ce système.

5.4.2 Modèle de charge

Pour déterminer si notre système est capable de détecter des nœuds malicieux, nous réalisons des simulations en suivant un modèle stochastique. La mesure de l'efficience de notre système se fera en utilisant un modèle déterministe.

Modèle stochastique

Dans cette partie, nous considérons seulement la version flexible de notre système de réputation et nous prenons pour acquis que les résultats obtenus pour cette version du système le sont aussi pour la version binaire. Car la différence entre les deux systèmes résident dans la façon de noter les différentes variables. Ce qui n'est pas une contrainte dans le fait de détecter ou non des requêtes malicieuses. Nos paramètres étant représentés suivant des intervalles de données, nous injectons des variables pseudo-aléatoires choisies par l'ordinateur et délimitées selon une plage de valeur donnée. Les intervalles de choix sont construits en élargissant les paramètres acceptables par le système suivant trois niveaux de flexibilité. Nous avons élargi l'intervalle à 25 %, 50 % et 75 % pour agrandir progressivement le champ de choix pour les variables. Ensuite nous observons le comportement du protocole AODV vis-à-vis des requêtes reçues. La durée des différents scénarios de simulation varie de 100s à 1000s. La figure 5.1 démontre que le taux de requêtes acceptées par le protocole est inférieur à 100 %. Cette observation nous permet de constater que le système de réputation que nous présentons, permet de supprimer les requêtes ayant des informations erronées. Ces requêtes proviennent de nœuds ayant mentis sur les informations qu'elles ont publiées. Nous constatons que le taux de nœuds acceptés dépend du pourcentage de relâchement des intervalles de paramètres. Il est tout à fait logique qu'avec une flexibilité de 25 % il y ait plus de requêtes acceptées qu'à 50 % et 75 %. L'intervalle de choix étant rétréci, il y a plus de chance de choisir les variables qui respectent les paramètres attendues.

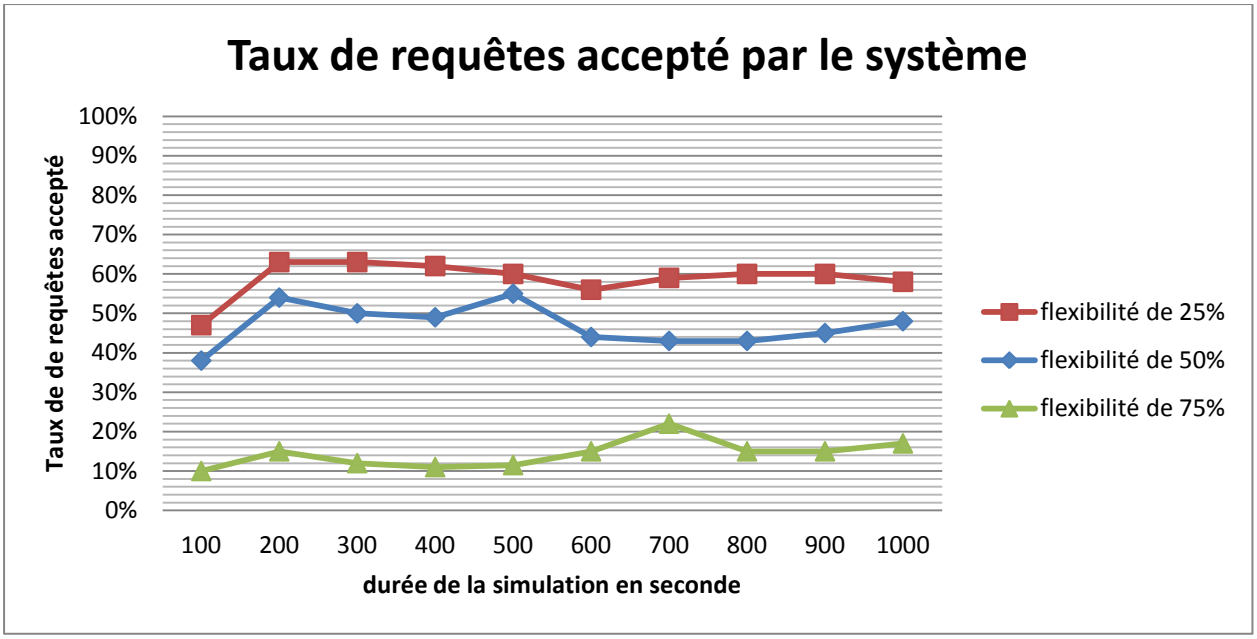

Figure 5.1: Taux de requête accepté par le protocole AODV selon le temps de simulation

5.4.2.1 Modèle déterministe

Le modèle déterministe nous permet d'injecter dans le système des valeurs connues à l'avance. De ce fait, nous prédéterminons le pourcentage de requêtes malicieuses envoyés et nous observons le comportement du système. La figure 5.2 montre que le taux de requêtes supprimées est sensiblement égal du taux de requêtes malicieuses injectées dans le système. Même si la détection n'est pas parfaite, en moyenne 85% des requêtes malicieuses sont supprimées. Ce résultat nous mène à la conclusion que notre système de réputation est capable de détecter sensiblement toutes les requêtes ayant publiées des informations erronées.

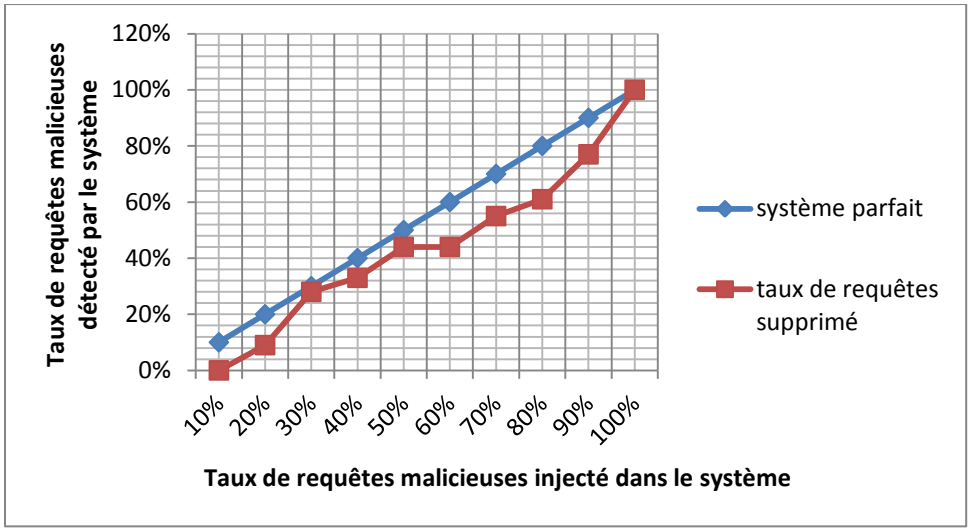

Figure 5.2: Taux de requêtes supprimé par rapport aux taux de requêtes malicieuses

Dans ce chapitre, nous avons présenté l'évaluation des performances de notre système de réputation. Pour réaliser nos simulations, nous avons modifié l'entête du protocole AODV pour insérer nos variables. De plus nous avons inclus dans la fonction de réception des requêtes notre système de réputation. Dans notre plan d'expérience, nous avons considéré le modèle stochastique qui nous a permis de conclure que notre système est bien fonctionnel, car nous nous sommes rendu compte que toutes les requêtes envoyées n'étaient pas reçues, car certaines comportaient des variables erronées qui ont été détectées par le système de réputation. De plus ces requêtes ont été supprimées. Ce qui nous montre aussi que notre système permet de rejeter tous les nœuds ayant fourni des variables erronées. Dans un second temps, nous avons réalisé des simulations avec un modèle déterministe. Notre objectif était de nous rassurer que notre système est capable de détecter tous les nœuds malicieux du système. Les résultats de simulation nous montre la détection se fait à 85 %. Ce qui est un chiffre assez satisfaisant. Nous pouvons donc conclure que notre système permet de détecter et d'éjecter les requêtes malicieuses, mais aussi qu'il est efficient.

CHAPITRE 6

CONCLUSIONS ET DISCUSSIONS

Les réseaux ad-hoc véhiculaires constituent un nouveau type de réseaux issus des réseaux ad-hoc mobiles (MANETs). Leur particularité vient de ce qu'ils permettent la communication entre les véhicules sur les routes. Cette communication peut être réalisée autant dans une topologie à infrastructure avec des stations de base et des RSU (Road Side Unit) que dans une topologie ad-hoc dans laquelle les nœuds communiquent les uns avec les autres sans besoin de tiers d'aide à la communication. Le partage d'information entre les véhicules permet d'éviter certaines situations tels que des accidents, des situations de trafics aux heures de pointe par exemple, grâce à ces informations, les véhicules peuvent s'informer les uns des autres sur l'état de la route et ainsi éviter des situations malencontreuses aux automobilistes. L'implémentation des VANETs donne lieu à d'autres applications telles que la maintenance à distance, le payement et l'accès à des services à distance. Il est même aussi possible de penser à des applications de confort telles que les jeux en réseaux, le téléchargement d'applications multimédia comme la musique ou les séquences vidéo. En d'autres termes, les VANETs permettent de rendre le système de transport plus fiable et sécuritaire tout en permettant aux usagers de la route de voyager dans des conditions agréables.

Le problème principal des VANETs réside dans le fait que les informations qui sont échangées entre les véhicules sont des données informatiques donc susceptible de subir tout type d'attaque. Que ce soit une attaque sur les données partagées par exemple en modifiant les informations c'est-à-dire l'intégrité même des données, soit en écoutant et en collectant les informations à propos des usagers de façon à les utiliser par la suite à mauvais escient, soit en injectant dans le réseau des informations erronées de façon à modifier le comportement des usagers de la route ou encore en perpétrant une attaque sur le réseau sous-jacent , c'est-à-dire en empêchant la communication entre les véhicules par exemple par une attaque de déni de service qui a pour objectif de paralyser le réseau.

Les solutions pour résoudre la question de la sécurité des réseaux VANETs ont été proposées par les chercheurs, les concepteurs automobiles et même les concepteurs de la technologie des VANETs. L'authentification des véhicules, la sécurisation des messages échangés par des

méthodes cryptographiques sont des solutions qui sécurisent les VANETS. Malheureusement toutes ces solutions résolvent toujours partiellement le problème de la sécurisation des VANETs. Dans la plupart des cas, elles permettent de détecter les nœuds malicieux, mais elles ne donnent pas le moyen de mettre ces derniers hors d'état de nuire par exemple en les excluant des communications réseaux. Dans notre travail, nous avons décidé de nous placer à la frontière des réseaux VANETs dans le cas d'une topologie de réseau ad-hoc. Nous mettons en place un système de réputation qui permettra de filtrer les véhicules réputés malicieux, c'est-à-dire des nœuds ayant fourni des variables erronées. Les véhicules ont le choix de communiquer seulement avec d'autres véhicules en qui ils ont confiance, car ceux-ci ont été définis honnêtes par le système de réputation embarqué sur chaque nœud. Ainsi dans notre mémoire, nous avons présenté notre système de réputation SSVR, il a été conçu pour doter les véhicules d'un système de réputation de façon à aider ces derniers à prendre la bonne décision pour le choix de leur partenaire de communication et aussi à construire une certaine confiance vis-à-vis de leurs éventuels partenaires de communication. Ce système est divisé en plusieurs fonctions qui analysent les différentes variables de la trame beacon envoyée par le nœud visiteur. Le système fonctionne selon un algorithme qui utilise non seulement les informations collectées localement mais aussi les observations réalisées par les nœuds voisins pour construire un score de réputation fiable. L'évaluation des performances de ce système a été réalisée en considérant une attaque d'illusion, pour une application d'avertissement de collision. L'attaque d'illusion a pour caractéristique d'envoyer de faux messages aux véhicules voisins de façon à causer des accidents et à changer le comportement des automobilistes dans des situations particulières. Car les variables publiées par le nœud visiteur telles que sa position géographique, sa vitesse, son accélération, sont utilisées pour décider de l'action à mener lorsqu'un évènement survient sur la route. Les résultats de simulation ont prouvé l'efficacité et la pertinence de notre système. Et pourtant, ce système nécessite encore de nombreuses améliorations.

Pour conclure ce mémoire nous présentons les difficultés rencontrées, les limites et les contributions suivront et en fin nous présentons les recommandations sur des voies de recherche ultérieures qui pourraient susciter de l'intérêt.

6.1 Difficultés rencontrées

Le système de réputation SSVR, tel que nous l'avons proposé, permet de réaliser des analyses sur les requêtes reçues. Cela permet donc de filtrer à l'entrée du réseau les véhicules qui mentent sur les variables qu'ils fournissent à leur voisinage. Grâce à ce filtrage, plusieurs attaques peuvent être évitées, par exemple, l'attaque du mensonge sur la position pour laquelle un véhicule peut prétendre être à une position alors que ce n'est pas le cas, afin de créer l'illusion d'un véhicule à cette position. Les attaques de Sybil sont reconnues d'être basé sur une multitude de faux nœuds qui prétendent exister alors qu'ils ne sont que virtuels. En vérifiant les informations annoncées par ce type de nœuds, on peut éviter ce type d'attaque. L'attaque d'illusion où l'adversaire fournit des variables erronées afin de changer le comportement des automobilistes, créant des situations pouvant mener à des accidents ou à des troubles de la circulation. Ce travail ne s'est pas fait sans difficultés, en effet, nous avons rencontré plusieurs embuches; dans un premier temps les difficultés inhérentes à la construction d'un système de réputation. Il a été difficile de concevoir l'architecture globale de notre système avec la prise en considération de tous les modules et de toutes les listes. Nous avons eu de la difficulté à définir le système de notation à attribuer à chacune des métriques reliées aux variables fournies par les nœuds émetteurs. Il a aussi été difficile de définir correctement la façon dont nous devions inclure les témoignages provenant des voisins. Le choix du seuil à fixer pour la prise de décision a aussi constitué une difficulté. Une fois l'architecture du système conçus, le modèle mathématique et l'algorithme écris, nous avons eu du mal à implémenter notre système de manière à faire une évaluation de performance pertinente par des simulations. Pour cela, nous avons dû modifier l'implémentation du protocole AODV dans le simulateur NS-2. Cette tâche n'a pas été aisée, car il nous a fallu comprendre le fonctionnement et l'implémentation de ce protocole sous NS-2. Il demeure la question de savoir de façon pratique comment notre système pourrait être implémenté sur les véhicules.

6.2 Limites

Le système de réputation que nous proposons comporte plusieurs limites : Ce système n'est capable de sécuriser que les applications qui sont relatives à la sécurité (safety related applications) des routes, car ces dernières exploitent les variables que nous testons. Toutes les

attaques perpétrées sur les autres applications restent donc sans défense avec notre système. Si plusieurs nœuds s'associent pour perpétrer des attaques, il est difficile de les en empêcher avec notre système de réputation. Le système devrait pouvoir prendre en compte l'environnement dans lequel le véhicule se trouve : est-ce une autoroute, le centre-ville, un quartier résidentiel, une zone rurale, dans la version actuelle cette particularité n'est pas prise en compte. Le système SSVR ne respecte pas la vie privée des usagers dans la mesure où l'identifiant de tout nœud voisin est conservé par le nœud hôte à moins de mettre en place un système d'utilisation d'identifiant temporaire arbitraire mais unique. Un nœud malicieux qui arrive à infiltrer le réseau pourra collecter des informations sur les autres nœuds. De plus, tel que présenté, ce système ne permet pas de gérer le cas des véhicules qui sont en situation de panne, il ne fait pas une différence entre les types de véhicules sur la chaussée, par exemple la différence entre les gros porteurs et les voitures de promenade, ou encore les voitures de police et les véhicules d'urgence telles que les ambulances. Les simulations que nous avons réalisées ne permettent pas d'évaluer les effets de notre système de réputation sur les performances du réseau.

6.3 Contributions

Notre système de réputation contient tous les composants que doivent comporter un système de réputation. En effet, le système que nous proposons, analyse les paquets provenant de l'émetteur. Pour conserver les observations faites à propos des nœuds visiteurs et des nœuds voisins, nous avons défini les différentes listes que nous avons mentionnées dans notre architecture. Il s'agit des listes des voisins, des listes noires, des listes d'historiques, des listes de réputation indirecte et des listes rouges. Ces différentes listes permettent de conserver les informations importantes de notre système. Les fonctions d'analyse des différentes variables, le module d'agrégation du score local de réputation, le module d'agrégation du score global de réputation, le module de prise en compte de l'historique et le module de réhabilitation joue le rôle de processus de traitement et enfin, notre système dispose d'un module de prise de décision. À l'issue de notre travail, nous avons apporté des contributions considérables. Notre système de réputation permet non seulement de détecter les adversaires mais aussi de supprimer les messages provenant de ces adversaires et ainsi de les éjecter du réseau, alors que la plupart des systèmes de sécurisation des VANETs permettent de détecter les adversaires potentiels mais ne permettent pas de les éjecter du réseau [101]. Notre système est un système générique qui peut être adapté à

toutes les applications pour lesquelles les variables fournies par les nœuds voisins peuvent modifier le comportement des automobilistes. Quelques-unes de ces applications sont : les applications d'avertissement des conditions de la route, les applications d'urgence de freinage, les applications de détection d'intersection. Globalement notre système de réputation est applicable sur les applications dites "safety related applications". Le système que nous proposons introduit de la flexibilité ce qui permettra aux utilisateurs de ce système le personnaliser selon les contraintes auxquelles ils devront faire face. Nous avons proposé un système à deux niveaux : le niveau binaire qui est rigide et le niveau flexible qui peut être plus ou moins rigoureux selon les besoins de l'utilisateur. Notre système en plus de détecter les adversaires potentiels, de les éjecter du réseau, il permet aussi de réhabiliter les anciens adversaires qui se comportent maintenant de façon exemplaire. Notre système permet aussi d'agréger toutes les notes obtenues en local et prend aussi en considération les témoignages faites par les voisins. Nous avons été capable d'effectuer des modifications sur le protocoles AODV et nous avons réussi à faire des simulations réalistes alors que la plupart des articles publiées à propos de la réputation n'intègrent pas des résultats de simulations [92, 101].

6.4 Les travaux futurs

Dans nos travaux futurs, nous nous attèlerons à corriger les limites que nous avons soulevé dans les paragraphes précédents. Nous réaliserons des simulations de façon à évaluer les performances du réseau. Ensuite, nous tenterons d'améliorer notre système pour prendre en considération l'environnement dans lequel les nœuds évoluent en définissant des métriques qui tiennent compte de l'environnement dans lequel le nœud évolue et aussi de sa situation sur la chaussée. Nous aimerons aussi rendre notre système dynamique de façon à ce qu'il s'adapte automatiquement selon la situation ou bien l'application en cours. Ainsi, si c'est une application pour laquelle la vitesse du véhicule est très importante, la note de cette variable aura un poids plus élevé et sera plus sensible que les autres variables.

RÉFÉRENCES

[1] G. Jyoti and M. S. Gaur, "Security of self-organizing networks MANET, WSN, WMN, VANET," Auerbach ed: CRC Press, 2010.

[2] Y. wang and F. Li, *Vehicular Ad Hoc Networks*. London: Springer-Verlag 2009.

[3] V. S. Yadav, S. Misra, and M. Afaque, "Security of self-organizing networks," ed, 2010.

[4] S. N. Pathak and U. Shrawankar, "Secured Communication in Real Time VANET," in *Emerging Trends in Engineering and Technology (ICETET), 2009 2nd International Conference on*, 2009, pp. 1151-1155.

[5] H. Hartenstein and Kenneth P. Laberteaux, "A tutorial survey on vehicular ad hoc networks," *IEEE Communications Magazine*, 2008.

[6] A. Stampoulis and Z. Chai, "A Survey of Security in Vehicular Networks," 2007.

[7] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges," *Springer Science*, 2010.

[8] T. Leinmuller, R. K. Schmidt, E. Schoch, A. Held, and G. Schafer, "Modeling Roadside Attacker Behavior in VANETs," in *GLOBECOM Workshops, 2008 IEEE*, New Orleans, LO, 2008, pp. 1 - 10

[9] YasserToor, P. Muhlethaler, A. Laouiti, and A. d. l. fortelle, "Vehicle Ad Hoc Networks: Applications And Related Technical Issues," *IEEE Communications*, vol. 10, 2008.

[10] M. Raya and J. P. Hubaux, "The Security of Vehicular Ad Hoc Networks," in *Security in Ad hoc and Sensor Networks (SASN)*, 2005.

[11] G. Yan, B. B. Bista, D. B. Rawat, and E. F. Shaner, "General Active Position Detectors Protect VANET Security," in *Broadband and Wireless Computing, Communication and Applications (BWCCA)*, 2011, pp. 11-17

[12] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks," *IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS*, vol. 21, 2010.

[13] R. MERAIHI, S.-M. SENOUCI, D.-E. MEDDOUR, and M. JERBI, "Vehicle-to-Vehicle Communications: Applications and Perspectives," in *Wireless Ad Hoc and Sensor Networks*, ed, 2008.

[14] A. L. Svenson and J. Mueller, "VEHICLE SAFETY COMMUNICATIONS FOR COMMERCIAL VEHICLES: ISSUES AFFECTING DEPLOYMENT OF VEHICLE-TO-VEHICLE COMMUNICATIONS FOR HEAVY VEHICLES."

[15] M. Schagrin. (2012, 2013-17-01). *Vehicle-to-Infrastructure (V2I) Communications for Safety*. Available: http://www.its.dot.gov/research/v2i.htm

[16] J. T. Issac, S.Zeadally, and J. S. Camara, "Security attacks and solutions for vehicular ad hoc networks," *IET Communication*, vol. 4, pp. 894-903, 2010-04-30 2010.

[17] X. Yang, L. Liu, N. H. Vaidya, and F. Zhao, "A vehicle-to-vehicle communication protocol for cooperative collision warning," in *Mobile and Ubiquitous Systems: Networking and Services, 2004. MOBIQUITOUS 2004. The First Annual International Conference on*, 2004, pp. 114-123.

[18] M. Torrent-Moreno, P. Santi, and H. Hartenstein, "Fair sharing of bandwidth in VANETs," presented at the Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks, Cologne, Germany, 2005.

[19] G. Samara, W. A. H. Al-Salihy, and R. Sures, "Security issues and challenges of Vehicular Ad Hoc Networks (VANET)," in *New Trends in Information Science and Service Science (NISS), 2010 4th International Conference on*, 2010, pp. 393-398.

[20] M. Raya, P. Papadimitratos, and J. P. Hubaux, "Securing vehicular communications," *Wireless Communications, IEEE,* vol. 13, pp. 8-15, 2006.

[21] F. K. Karnadi, M. Zhi Hai, and L. Kun-chan, "Rapid generation of realistic mobility models for VANET," in *Wireless Communications and Networking Conference, 2007.WCNC 2007. IEEE*, 2007, pp. 2506-2511.

[22] C. Gosman, C. Dobre, and V. Cristea, "A security protocol for vehicular distributed systems," in *Symbolic and Numeric Algorithms for Scientific Computing (SYNASC), 2010 12th International Symposium on*, 2010, pp. 321-327.

[23] B. Parno and A. Perrig, "Challenges in securing vehicular networks," in *Workshop on Hot Topics in Networks (HotNets-IV)*, 2005.

[24] G. Samara, W. A. H. Al-Salihy, and R. Sures, "Security analysis of vehicular ad hoc nerworks (VANET)," in *Network Applications Protocols and Services (NETAPPS)*, 2010, pp. 55-60.

[25] C. D. Wang and J. P. Thompson, "Apparatus and method for motion detection and tracking of objects in a region for collision avoidance utilizing a real-time adaptive probabilistic neural network," 5613039, 1997.

[26] B. Fouch. Available: http://safety.fhwa.dot.gov/roadway_dept/crash_facts/

[27] U. Delprato, M. Cristaldi, and A. Gambardella, "Sharing emergency information between cmergency control centres: the troject REACT " in *International Congress on Environmental Modelling and Software Integrating Sciences and Information Technology for Environmental Assessment and Decision Making*, 2008.

[28] "Identify intelligent vehicle safety applications enabled by DSRC," U.S. National Highway Traffic Safety Administration2005.

[29] H. T. Cheng, H. Shan, and W. Zhuang, "Infotainment and road safety service support in vehicular networking: from a communication perspective," *Mechanical Systems and Signal Processing*, 2010.

[30] M. Segata and R. L. Cigno, "Models and Performance of VANET based Emergency Braking," TRENTO2011.

[31] K. V. N. Kavitha, A. Bagubali, and L. Shalini, "V2V Wireless Communication Protocol for Rear-end Collision Avoidance on Highways with Stringent Propagation Delay," in *Advances in Recent Technologies in Communication and Computing, 2009. ARTCom '09. International Conference on*, 2009, pp. 661-663.

[32] K. Dresner and P. Stone, "A multiagent approach to autonomous intersection management," *J. Artif. Int. Res.*, vol. 31, pp. 591-656, 2008.

[33] F. Kargl, Z. Ma, and E. Schoch, "Security engineering for vanets," in *4th Wksp. Embedded Sec. in Cars*, 2006.

[34] S. Biswas, Mis, x030C, ic, x, and J., "Proxy signature-based RSU message broadcasting in VANETs," in *Communications (QBSC), 2010 25th Biennial Symposium on*, 2010, pp. 5-9.

[35] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, M. Zhendong, F. Kargl, A. Kung, and J. P. Hubaux, "Secure vehicular communication systems: design and architecture," *Communications Magazine, IEEE*, vol. 46, pp. 100-109, 2008.

[36] A. Stampoulis and C. Z., "Survey of security in vehicular networks," in *Project CPSC*, 2007.

[37] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in VANETs," presented at the Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks, Philadelphia, PA, USA, 2004.

[38] F. Armknecht, A. Festag, D. Westhoff, and K. Zeng, "Cross-layer privacy enhancement and non-repudiation in vehicular communication," *Communication in Distributed Systems (KiVS), 2007 ITG-GI Conference*, pp. 1-12, 2007.

[39] Q. Yi and N. Moayeri, "Design of secure and application-oriented VANETs," in *Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE*, 2008, pp. 2794-2799.

[40] K. Plossl, T. Nowey, and C. Mletzko, "Towards a security architecture for vehicular ad hoc networks," in *Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on*, 2006, p. 8 pp.

[41] C.-T. Li, M.-S. Hwang, and Y.-P. Chu, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks," *Computer Communications*, vol. 31, pp. 2803-2814, 2008.

[42] H. Moustafa, G. Bourdon, and Y. Gourhant, "Providing authentication and access control in vehicular network environment," in *Security and Privacy in Dynamic Environments*. vol. 201, S. FischerHubner, K. Rannenberg, L. Yngstrom, and S. Lindskog, Eds., ed New York: Springer, 2006, pp. 62-73.

[43] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, pp. 39-68, 2007.

[44] T. Zhou, R. R. Choudhury, P. Ning, and K. Chakrabarty, "Privacy-preserving detection of sybil attacks in vehicular ad hoc networks," in *Mobile and Ubiquitous Systems:*

Networking & Services, 2007. MobiQuitous 2007. Fourth Annual International Conference on, 2007, pp. 1-8.

[45] K. El Defrawy and G. Tsudik, "PRISM: Privacy-friendly routing in suspicious MANETs (and VANETs)," in *Network Protocols, 2008. ICNP 2008. IEEE International Conference on*, 2008, pp. 258-267.

[46] C. Laurendeau and M. Barbeau, "Threats to Security in DSRC/WAVE," *Ad-Hoc, Mobile, and Wireless Networks*, pp. 266-279, 2006.

[47] Y. Hao, Y. Cheng, and K. Ren, "Distributed key management with protection against RSU compromise in group signature based VANETs," in *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*, 2008, pp. 1-5.

[48] K. Papapanagiotou, G. F. Marias, and P. Georgiadis, "A certificate validation protocol for vanets," in *Globecom Workshops, 2007 IEEE*, 2007, pp. 1-9.

[49] N. Vighnesh, N. Kavita, S. R. Urs, and S. Sampalli, "A novel sender authentication scheme based on hash chain for Vehicular Ad-Hoc Networks," in *Wireless Technology and Applications (ISWTA), 2011 IEEE Symposium on*, 2011, pp. 96-101.

[50] F. Sabahi, "The Security of Vehicular Adhoc Networks," in *Computational Intelligence, Communication Systems and Networks (CICSyN), 2011 Third International Conference on*, 2011, pp. 338-342.

[51] N. Ben Salem and J. P. Hubaux, "Securing wireless mesh networks," *Wireless Communications, IEEE*, vol. 13, pp. 50-55, 2006.

[52] B. Xiao, B. Yu, and C. Gao, "Detection and localization of sybil nodes in VANETs," in *International Conference on Mobile Computing and Networking: Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks*, 2006, pp. 1-8.

[53] V. Igure and R. Williams, "Taxonomies of attacks and vulnerabilities in computer systems," *Communications Surveys & Tutorials, IEEE*, vol. 10, pp. 6-19, 2008.

[54] T. Leinmuller, R. K. Schmidt, E. Schoch, A. Held, and G. Schafer, "Modeling roadside attacker behavior in vanets," in *GLOBECOM Workshops, 2008 IEEE*, 2008, pp. 1-10.

[55] A. Hussain, J. Heidemann, and C. Papadopoulos, "A framework for classifying denial of service attacks," in *Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications*, 2003, pp. 99-110.

[56] K. S. Killourhy, R. A. Maxion, and K. M. Tan, "A defense-centric taxonomy based on attack manifestations," in *Dependable Systems and Networks, 2004 International Conference on*, 2004, pp. 102-111.

[57] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," *ACM SIGCOMM Computer Communication Review*, vol. 34, pp. 39-53, 2004.

[58] I. Aad, J. P. Hubaux, and E. W. Knightly, "Impact of Denial of Service Attacks on Ad Hoc Networks," *Networking, IEEE/ACM Transactions on*, vol. 16, pp. 791-802, 2008.

[59] J. Blum and A. Eskandarian, "The threat of intelligent collisions," *IT professional*, vol. 6, pp. 24-29, 2004.

[60] I. Ahmed Soomro, H. Hasbullah, and J.-l. Ab Manan, "Denial of Service (DOS) Attack and Its Possible Solution in VANET," 2010.

[61] J. M. d. Fuentes, A. I. González-Tablas, and A. Ribagorda, "Overview of security issues in Vehicular Ad-hoc Networks," 2010.

[62] D. Ren, S. Du, and H. Zhu, "A novel attack tree based risk assessment approach for location privacy preservation in the VANETs," in *Communications (ICC), 2011 IEEE International Conference on*, 2011, pp. 1-5.

[63] T. W. Chim, S. Yiu, L. C. Hui, and V. O. Li, "Security and privacy issues for inter-vehicle communications in vanets," in *Sensor, Mesh and Ad Hoc Communications and Networks Workshops, 2009. SECON Workshops' 09. 6th Annual IEEE Communications Society Conference on*, 2009, pp. 1-3.

[64] C. Harsch, A. Festag, and P. Papadimitratos, "Secure Position-Based Routing for VANETs," in *Vehicular Technology Conference, 2007. VTC-2007 Fall. 2007 IEEE 66th*, 2007, pp. 26-30.

[65] C. Jung, C. Sur, Y. Park, and K.-H. Rhee, "A Robust Conditional Privacy-Preserving Authentication Protocol in VANET," in *Security and Privacy in Mobile Information and Communication Systems*. vol. 17, A. Schmidt and S. Lian, Eds., ed: Springer Berlin Heidelberg, 2009, pp. 35-45.

[66] E. Fonseca and A. Festag, "A survey of existing approaches for secure ad hoc routing and their applicability to VANETS," *NEC network laboratories*, 2006.

[67] L. Ertaul and S. Mullapudi, "The Security Problems of Vehicular Ad Hoc Networks (VANETs) and Proposed Solutions in Securing their Operations," in *The 2009 International Conference on Wireless Networks ICWN*, 2009.

[68] L. Nai-Wei and T. Hsiao-Chien, "Illusion Attack on VANET Applications - A Message Plausibility Problem," in *Globecom Workshops, 2007 IEEE*, 2007, pp. 1-8.

[69] S. U. Rahman and H. Falaki, "Security & Privacy for DSRC-based Automotive Collision Reporting," ed.

[70] M. Koubek, S. Rea, and D. Pesch, "Event Suppression for Safety Message Dissemination in VANETs," in *Vehicular Technology Conference (VTC 2010-Spring), 2010 IEEE 71st*, 2010, pp. 1-5.

[71] Y. Toor, P. Muhlethaler, and A. Laouiti, "Vehicle Ad Hoc networks: applications and related technical issues," *Communications Surveys & Tutorials, IEEE*, vol. 10, pp. 74-88, 2008.

[72] I. A. Sumra, H. Hasbullah, M.-u.-R. Jamalul-lail, and B. S. Iskandar, "Trust and Trusted Computing in VANET," *Computer Science*, vol. 1, 2011.

[73] G. Guette and C. Bryce, "Using tpms to secure vehicular ad-hoc networks (vanets)," *Information Security Theory and Practices. Smart Devices, Convergence and Next Generation Networks*, pp. 106-116, 2008.

[74] S. K. Dhurandher, M. S. Obaidat, A. Jaiswal, A. Tiwari, and A. Tyagi, "Securing vehicular networks: A reputation and plausibility checks-based approach," in *GLOBECOM Workshops (GC Wkshps), 2010 IEEE*, 2010, pp. 1550-1554.

[75] R. R. Brooks, S. Sander, D. Juan, and J. Taiber, "Automobile security concerns," *Vehicular Technology Magazine, IEEE*, vol. 4, pp. 52-64, 2009.

[76] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "Amoeba: Robust location privacy scheme for vanet," *Selected Areas in Communications, IEEE Journal on*, vol. 25, pp. 1569-1589, 2007.

[77] F. Dötzer, "Privacy issues in vehicular ad hoc networks," in *Privacy Enhancing Technologies*, 2006, pp. 197-209.

[78] V. Pathak, D. Yao, and L. Iftode, "Securing location aware services over VANET using geographical secure path routing," in *Vehicular Electronics and Safety, 2008. ICVES 2008. IEEE International Conference on*, 2008, pp. 346-353.

[79] A. Kapadia, N. Triandopoulos, C. Cornelius, D. Peebles, and D. Kotz, "AnonySense: Opportunistic and privacy-preserving context collection," *Pervasive Computing*, pp. 280-297, 2008.

[80] P. Papadimitratos, L. Buttyan, J.-P. Hubaux, F. Kargl, A. Kung, and M. Raya, "Architecture for secure and private vehicular communications," in *Telecommunications, 2007. ITST'07. 7th International Conference on ITS*, 2007, pp. 1-6.

[81] F. Li and J. Wu, "A Winning-Probability-based Incentive Scheme in Vehicular Networks," in *Proc. of IEEE International Conference on Network Protocols (ICNP), poster abstract*, 2008.

[82] D. Wu, J. Cao, Y. Ling, J. Liu, and L. Sun, "Routing Algorithm Based on Multi-Community Evolutionary Game for VANET," *Journal of Networks*, vol. 7, pp. 1106-1115, 2012.

[83] A. P. Bernia, "Reliable and Secure Geocasting in VANETs," University of Ottawa, 2012.

[84] N. Liu, M. Liu, J. Cao, G. Chen, and W. Lou, "When Transportation Meets Communication: V2P over VANETs," in *Distributed Computing Systems (ICDCS), 2010 IEEE 30th International Conference on*, 2010, pp. 567-576.

[85] I. P. W. Group, "VSC project," *Dedicated short range communications (DSRC)*, 2003.

[86] M. Schulze, "Promote-Chauffeur," *Final Report, EU Telematics Applications*, 1999.

[87] T. E. Anderson, D. E. Culler, and D. Patterson, "A case for NOW (networks of workstations)," *Micro, IEEE*, vol. 15, pp. 54-64, 1995.

[88] D. Reichardt, M. Miglietta, L. Moretti, P. Morsink, and W. Schulz, "CarTALK 2000: Safe and comfortable driving based upon inter-vehicle-communication," in *Intelligent Vehicle Symposium, 2002. IEEE*, 2002, pp. 545-550.

[89] "TPM Main : Part 1 Design Principles," 29 March 2006 2006.

[90] A. Studer, F. Bai, B. Bellur, and A. Perrig, "Flexible, extensible, and efficient VANET authentication," in *Proceedings of the 6th Annual Conference on Embedded Security in Cars (escar 2008)*, 2008.

[91] J. Petit and Z. Mammeri, "Analysis of authentication overhead in vehicular networks," in *Wireless and Mobile Networking Conference (WMNC), 2010 Third Joint IFIP*, 2010, pp. 1-6.

[92] F. Dotzer, L. Fischer, and P. Magiera, "Vars: A vehicle ad-hoc network reputation system," in *World of Wireless Mobile and Multimedia Networks, 2005. WoWMoM 2005. Sixth IEEE International Symposium on a*, 2005, pp. 454-456.

[93] M. Raya, A. Aziz, and J.-P. Hubaux, "Efficient secure aggregation in VANETs," in *Proceedings of the 3rd international workshop on Vehicular ad hoc networks*, 2006, pp. 67-75.

[94] M. Rahbari and M. A. J. Jamali, "EFFICIENT DETECTION OF SYBIL ATTACK BASED ON CRYPTOGRAPHY IN VANET."

[95] A. Khalili, J. Katz, and W. A. Arbaugh, "Toward secure key distribution in truly ad-hoc networks," in *Applications and the Internet Workshops, 2003. Proceedings. 2003 Symposium on*, 2003, pp. 342-346.

[96] S. Buchegger, J. Mundinger, and J.-Y. Le Boudec, "Reputation systems for self-organized networks," *Technology and Society Magazine, IEEE*, vol. 27, pp. 41-47, 2008.

[97] S. Marti and H. Garcia-Molina, "Taxonomy of trust: Categorizing P2P reputation systems," *Computer Networks*, vol. 50, pp. 472-484, 2006.

[98] P. L. Mazenc, "Système de réputation préservant la vie privée," in *3ième édition Atelier Protection de la vie privée*, 2012.

[99] P. Resnick and R. Zeckhauser, "Trust among strangers in Internet transactions: Empirical analysis of eBay's reputation system," 2002.

[100] A. Josang, "Trust-based decision making for electronic transactions," in *Proceedings of the Fourth Nordic Workshop on Secure Computer Systems (NORDSEC'99)*, 1999, pp. 496-502.

[101] R. K. Schmidt, T. Leinmüller, E. Schoch, A. Held, and G. Schäfer, "Vehicle behavior analysis to enhance security in vanets," in *Proceedings of 4th Workshop on Vehicle to Vehicle Communications (V2VCOM 2008)*, 2008.

[102] J. Barnett, *La réputation pierre angulaire d'une protection efficace contre les menaces*

[103] (10-12-2012). Available: http://en.wikipedia.org/wiki/Reputation_system

[104] P. Resnick, K. Kuwabara, R. Zeckhauser, and E. Friedman, "Reputation systems," *Communications of the ACM*, vol. 43, pp. 45-48, 2000.

[105] A. Srinivasan, J. Teitelbaum, and J. Wu, "DRBTS: distributed reputation-based beacon trust system," in *Dependable, Autonomic and Secure Computing, 2nd IEEE International Symposium on*, 2006, pp. 277-283.

[106] S. Buchegger and J. Le Boudec, "The effect of rumor spreading in reputation systems for mobile ad-hoc networks," in *WiOpt'03: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks*, 2003.

[107] S. Buchegger and J.-Y. Le Boudec, "Performance analysis of the CONFIDANT protocol," in *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing*, 2002, pp. 226-236.

[108] A. Abdul-Rahman and S. Hailes, "Supporting trust in virtual communities," in *System Sciences, 2000. Proceedings of the 33rd Annual Hawaii International Conference on*, 2000, p. 9 pp. vol. 1.

[109] A. Jsang and R. Ismail, "The beta reputation system," in *Proceedings of the 15th bled electronic commerce conference*, 2002, pp. 41-55.

[110] J. Douceur, "The sybil attack," *Peer-to-peer Systems*, pp. 251-260, 2002.

[111] K. Hoffman, D. Zage, and C. Nita-Rotaru, "A survey of attack and defense techniques for reputation systems," *ACM Computing Surveys (CSUR)*, vol. 42, p. 1, 2009.

[112] E. Pavlov, J. Rosenschein, and Z. Topol, "Supporting privacy in decentralized additive reputation systems," *Trust Management*, pp. 108-119, 2004.

[113] A. Ravoaja, "Mécanismes et architectures P2P robustes et incitatifs pour la réputation," PhD, Rennes-1, 2008.

[114] N. Borisov, "Computational puzzles as sybil defenses," in *Peer-to-Peer Computing, 2006. P2P 2006. Sixth IEEE International Conference on*, 2006, pp. 171-176.

[115] Available: http://en.wikipedia.org/wiki/Google_bomb

[116] G. Urdaneta, G. Pierre, and M. V. Steen, "A survey of DHT security techniques," *ACM Computing Surveys (CSUR)*, vol. 43, p. 8, 2011.

[117] A. Saroliya and V. Shrivastava, "Security problems and their upshots in routing protocols of DHT based overlay networks," *Journal of Theoretical and Applied Information Technology*, 2005.

[118] T. Reidemeister, K. Böhm, E. Buchmann, and P. A. Ward, "Man-in-the-middle attacks in distributed hash-tables," *IEEE Journal on Selected Areas in Communication*, 2006.

[119] I. Stoica, R. Morris, D. Karger, M. F. Kaashoek, and H. Balakrishnan, "Chord: A scalable peer-to-peer lookup service for internet applications," *ACM SIGCOMM Computer Communication Review*, vol. 31, pp. 149-160, 2001.

[120] M. S. Artigas, P. G. Lopez, J. P. Ahullo, and A. F. G. Skarmeta, "Cyclone: A novel design schema for hierarchical dhts," in *Peer-to-Peer Computing, 2005. P2P 2005. Fifth IEEE International Conference on*, 2005, pp. 49-56.

[121] A. Fiat, J. Saia, and M. Young, "Making chord robust to byzantine attacks," *Algorithms–ESA 2005*, pp. 803-814, 2005.

[122] L. Page, S. Brin, R. Motwani, and T. Winograd, "The PageRank citation ranking: bringing order to the web," 1999.

[123] L. Page, "Method for node ranking in a linked database," ed: Google Patents, 2001.

[124] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *International Conference on Mobile Computing and Networking: Proceedings of the 6 th annual international conference on Mobile computing and networking*, 2000, pp. 255-265.

[125] P. Michiardi and R. Molva, "Simulation-based analysis of security exposures in mobile ad hoc networks," in *European Wireless Conference*, 2002.

[126] A. Srinivasan, J. Teitelbaum, J. Wu, M. Cardei, and H. Liang, "Reputation-and-Trust-Based Systems for Ad Hoc Networks," *Algorithms and protocols for wireless and mobile ad hoc networks*, p. 375, 2009.

[127] S. Bansal and M. Baker, "Observation-based cooperation enforcement in ad hoc networks," *arXiv preprint cs/0307012*, 2003.

[128] R. Molva and P. Michiardi, "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," *Institute EurecomResearch Report RR-02-062*, 2001.

[129] Q. Ding, X. Li, M. Jiang, and X. Zhou, "Reputation-based trust model in vehicular ad hoc networks," in *Wireless Communications and Signal Processing (WCSP), 2010 International Conference on*, 2010, pp. 1-6.

[130] J. P. Hubaux, S. Capkun, and L. Jun, "The security and privacy of smart vehicles," *Security & Privacy, IEEE*, vol. 2, pp. 49-55, 2004.

[131] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of Misbehaving and Faulty Nodes in Vehicular Networks," *IEEE Journal on Selected Areas in Communications, Special Issue on Vehicular Networks*, vol. 25, pp. 1557-1568, 2007.

[132] M. Raya, A. Aziz, and J.-P. Hubaux, "Efficient secure aggregation in VANETs," presented at the Proceedings of the 3rd international workshop on Vehicular ad hoc networks, Los Angeles, CA, USA, 2006.

[133] G. Yan, S. Olariu, and M. C. Weigle, "Providing VANET security through active position detection," *Computer Communications*, vol. 31, pp. 2883-2897, 2008.

[134] G. Jyoti, G. M, and L. V, "Sybil Attack in VANETs," in *Security of Self-Organizing Networks*, ed: Auerbach Publications, 2010, pp. 269-294.

[135] T. Lei, Z. Yunshan, and T. Lie, "Improving GPS positioning precision by using optical encoders," in *Intelligent Transportation Systems, 2000. Proceedings. 2000 IEEE*, 2000, pp. 293-298.

[136] N.-W. Lo and H.-C. Tsai, "Illusion attack on vanet applications-a message plausibility problem," in *Globecom Workshops, 2007 IEEE*, 2007, pp. 1-8.

[137] C. V. S. C. Consortium, "Vehicle safety communications project: Task 3 final report: Identify intelligent vehicle safety applications enabled by DSRC," *National Highway Traffic Safety Administration, US Department of Transportation, Washington DC*, 2005.

[138] T. Issariyakul and E. Hossain, *Introduction to network simulator NS2*: Springer, 2011.

[139] M. A. Ramteke, "Realistic Simulation for Vehicular Ad-hoc Network Using ZigBee Technology," *International Journal of Engineering*, vol. 1, 2012.